Privatizing Censorship, Eroding Privacy
by Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong

Internet freedom around the world has declined for the fifth consecutive year, with more governments censoring information of public interest and placing greater demands on the private sector to take down offending content.

State authorities have also jailed more users for their online writings, while criminal and terrorist groups have made public examples of those who dared to expose their activities online. This was especially evident in the Middle East, where the public flogging of liberal bloggers, life sentences for online critics, and beheadings of internet-based journalists provided a powerful deterrent to the sort of digital organizing that contributed to the Arab Spring.

In a new trend, many governments have sought to shift the burden of censorship to private companies and individuals by pressing them to remove content, often resorting to direct blocking only when those measures fail. Local companies are especially vulnerable to the whims of law enforcement agencies and a recent proliferation of repressive laws. But large, international companies like Google, Facebook, and Twitter have faced similar demands due to their significant popularity and reach.

Surveillance has been on the rise globally, despite the uproar that followed the revelation of mass data collection by the U.S. National Security Agency (NSA) in 2013. Several democratic countries, including France and Australia, passed new measures authorizing sweeping surveillance, prompted in part by domestic terrorism concerns and the expansion of the Islamic State (IS) militant group. Bans on encryption and anonymity tools are becoming more common, with governments seeking access to encryption backdoors that could threaten digital security for everyone. Evidence that governments with poor human rights records are purchasing surveillance and malware technologies from Western companies like Hacking Team has fueled suspicions that these tools are being used to crack down on political dissidents.

In the Middle East, flogging, life sentences, and beheadings deterred the sort of digital organizing that contributed to the Arab Spring.

Nevertheless, activists, advocacy groups, and journalists have pushed back against deteriorating conditions for global internet freedom. In India, legal petitions against Section 66A of the Information Technology (IT) Act—a restrictive provision that was used to criminalize online speech, particularly on social media—succeeded when the Supreme Court declared the provision unconstitutional in March 2015. In Argentina, the Supreme Court protected intermediaries from pressure to preemptively censor third-party content. And in the United States, the June 2015 passage of the USA Freedom Act marked an incremental step toward surveillance reform after nearly two years of debate over NSA practices.

In more repressive settings where the potential for legislative change is limited, activists have had some success in using information and communication...
In September 2015, the Chinese government censored images of the cartoon character Winnie the Pooh, which internet users on the microblogging site Sina Weibo posted in an allusion to the image of President Xi Jinping in a military parade. The image was shared over 65,000 times before it was removed and became the most censored image on Sina Weibo that month.

technologies (ICTs) to hold government officials accountable for abuses. In Ethiopia, demands for the release of the Zone 9 bloggers, who were being tried on terrorism charges, garnered global attention under the #FreeZone9Bloggers hashtag, apparently contributing to the release of five of the nine defendants in July 2015. And in Saudi Arabia, the ubiquity of smartphones enabled activists to post documentation of human rights violations online, sparking public outrage and resulting in the dismissal of two government officials.

Of the 65 countries assessed, 32 have been on a negative trajectory since June 2014.

While the overall trajectory for internet freedom remains negative, the declines over the last year were less precipitous than in the past. The small victories described above are promising signs that the setbacks of recent years can be reversed, and that the fight for a free and open internet will continue even under the harshest conditions.

Tracking the Global Decline
To illuminate the nature of the principal threats in this rapidly changing environment, Freedom House conducted a comprehensive study of internet freedom in 65 countries around the world. This report, the sixth in its series, primarily focuses on developments that occurred between June 2014 and May 2015, although some more recent events were included in individual country narratives. Over 70 researchers, nearly all based in the countries they analyzed, contributed to the project by examining laws and practices relevant to the internet, testing the accessibility of select websites, and interviewing a wide range of sources.

Of the 65 countries assessed, 32 have been on a negative trajectory since June 2014. The most significant declines occurred in Libya, Ukraine, and France. Libya, torn by internal conflict, experienced a troubling increase in violence against bloggers, new cases of political censorship, and rising prices for internet and mobile phone services. Ukraine, amid its own territorial conflict and propaganda war with Russia, featured more prosecutions for content that was critical of the government’s policies, as well as increased violence from pro-Russian paramilitary groups against users who posted pro-Ukraine content in the eastern regions. France’s standing declined primarily due to problematic policies adopted in the aftermath of the Charlie Hebdo terrorist attack, such as restrictions on content that could be seen as “apology for terrorism,” prosecutions of users, and significantly increased surveillance.

China was the year’s worst abuser of internet freedom. As President Xi Jinping made “cyber sovereignty” one of the priorities of his tenure as leader of the Chinese Communist Party, internet users endured crackdowns on “rumors,” greater enforcement of rules against anonymity, and disruptions to the circumvention tools that are commonly used to bypass censorship. Though not entirely new, these measures were implemented with unprecedented intensity. Google, whose services were frequently interrupted in the past, was almost completely blocked. Veteran human rights defenders were jailed for online expression, including lawyer Pu Zhiqiang, who faces charges of “picking quarrels” in connection with 28 social media posts, and 70-year-old journalist Gao Yu, who was sentenced to seven years in prison for sending “state secrets” to a foreign website. Official censorship directives during the year suppressed online commen-
Syria and Iran were the second- and third-worst performers, respectively. Activists, bloggers, and citizen journalists in Syria continue to risk death at the hands of armed factions from across the political spectrum. In Iran, positive moves by President Hassan Rouhani and the ICT Ministry have led to greater bandwidth and the expansion of 3G services across all major networks. However, despite the president’s reformist rhetoric, major improvements to civil liberties remain blocked by the supreme leader and the country’s conservative establishment. Eight young people were sentenced to a combined 127 years in prison for antigovernment posts on Facebook in July 2014.

By contrast, 15 countries registered overall improvements. The year’s biggest gains occurred in Sri Lanka following the January 2015 elections. The new government unblocked previously inaccessible websites and ceased harassing and prosecuting internet users. Cuba also registered an improvement after the reestablishment of diplomatic relations with the United States, marking a potential opening for the ICT sector. The cost of public internet access, though still out of reach for most Cubans, was cut in half; the first public Wi-Fi connections were established; and online media began to adopt a more critical tone toward the authorities. And Zambia enjoyed a reduction in major restrictions on online content compared with the previous year—a trend that continued under the new government elected in January 2015.
The following is a selection of the topics that were subject to censorship in the 65 countries covered in Freedom on the Net. A country was deemed to censor a topic if it blocked relevant webpages, initiated takedown and deletion requests, or detained users who posted content on that topic.

**Criticism of Authorities:** A remarkable 47 of the 65 countries assessed censored criticism of the authorities, the military, or the ruling family. In Thailand—where expression of antiroyal sentiment is severely restricted—authorities blocked thousands of sites featuring poetry, plays, and online radio services. In Morocco, police detained 17-year old rapper Othman Atiq for three months after he criticized them in online videos. All countries in the Middle East and North Africa, and nearly all countries in sub-Saharan Africa, censored such criticism.

**Corruption:** Authorities in 28 countries sought to cover up accusations of corruption or misuse of public funds. In Sudan, a journalist was arrested after implicating high-level officials in a real estate scam. In July 2015, the Malaysian government blocked access to the UK-based whistle-blower site Sarawak Report over its coverage of bribery allegations linking the prime minister and a Sarawak state investment fund.

**Political Opposition:** Twenty-three countries censored the political opposition, including Ethiopia, which obstructed hundreds of social media pages, blogs, and diaspora-based opposition websites that were created to report on the May 2015 general elections. Such censorship is often very effective in ensuring that opposing views are rarely heard and helping the incumbent government to stay in power.

**Satire:** Authorities in 23 of the 65 countries assessed went to great lengths to muzzle ridicule and ironic commentary about public officials. A court in Bangladesh, for example, sentenced a 25-year-old to seven years in prison—the minimum under the amended ICT Act—for sharing a satirical song via his mobile phone. And an Iranian cartoonist was sentenced to 12 years of prison for posting an image in which she depicted members of parliament as animals (see page 11).

**Social Commentary:** Discussion on social issues—including economic conditions and cultural questions—was targeted for censorship in 20 of the countries assessed. In Venezuela, the majority of blocking activity pertained to information about the black-market dollar exchange rate; photos of long lines outside supermarkets were also subject to censorship. The Chinese authorities regulated stories about “one-night stands” in 2015. And in Indonesia, a young woman was sentenced to two months in prison after her social media complaint calling the city of Yogyakarta “uncivilized” went viral in March 2015.

**Blasphemy:** Twenty-one countries censored content that was considered insulting to religion. Blasphemy laws are often enforced selectively or arbitrarily to persecute religious minorities and serve political agendas. In Turkey, authorities censor content that is perceived as insulting to Islam, while offenses to other religions frequently go unchecked. Bahraini authorities are more likely to block alleged blasphemy of religious figures revered by the royal family and other Sunni Muslims than attacks on those sacred to the majority Shia population.

**Mobilization for Public Causes:** Sixteen of the countries in Freedom on the Net censored digital activism such as calls to protest, online petitions, or campaigns for social or political action. Authorities in Bahrain, Saudi Arabia, and the United Arab Emirates (UAE) censored human rights campaigners, while Russia blocked posts that called for protests after the court sentencing of opposition figure Aleksey Navalny. In 2014, the Saudi #Women2Drive campaign encouraged women to share videos and images of themselves behind the wheel to challenge a de facto ban on women drivers, but authorities blocked the campaign website.

**LGBTI Issues:** Fourteen countries targeted LGBTI (lesbian, gay, bisexual, transgender, and intersex) content for censorship on moral, religious, or other
Methods represented here are usually explicitly state-sanctioned, including blocking, content removal, and prosecutions. The chart does not consider extralegal pressures like violence, self-censorship, or cyberattacks, even where the state is believed to be responsible.

* Until Jan. 2015
In a new development, more governments are now pressuring companies and individuals to remove content, as opposed to simply blocking or filtering the relevant websites and services. While blocking and filtering are still widespread tactics, the growing use of circumvention tools and encryption has made them less effective, particularly if the goal is to block individual pages and not whole sites or platforms.

By contrast, content removal—including takedowns or deletions of specific webpages, blogs, videos, articles, and social media posts by tech companies, webmasters, and users—ensures that the material is restricted at the source. Even if the content is hosted abroad and the company in question is unwilling to take it down completely, they may decide to withdraw it from view in that country, particularly if the request is rooted in local laws. This remains problematic, however, since laws in many states do not meet international standards of free expression.

The approaches to content removal vary, and can include direct government requests to content hosts, threats and intimidation directed at individual users, or broad laws that compel companies to proactively monitor and delete content. But all of these methods have the effect of shifting the burden of censorship to private companies and citizens.

In total, authorities in 42 out of the 65 countries assessed required companies, site administrators, and users to restrict online content of a political, social, or religious nature, up from 37 the previous year. Governments have also grown more aggressive in presenting companies with ultimatums, threatening to revoke their operating licenses or block entire platforms if the specified content is not removed or hidden from view. This change was driven in part by the recent proliferation of laws that criminalize various types of online speech, adding force to the authorities’ removal requests.

The trend is apparent not just in the number of governments taking this approach, but also in the num-
number of removal requests received by technology companies. Several international firms such as Google, Facebook, and Twitter publish transparency reports that reveal the number of requests they receive each year and their compliance rate. Requests to Twitter from courts and government agencies around the world, for example, skyrocketed from 6 to 1,003 in the three years it has released data. Although companies in many developing markets are not very transparent about such data, interviews conducted by Freedom House indicate that requests are indeed increasing.

**Incentives Driving the Trend**

Governments are choosing content removal over blocking and filtering for several reasons. With the exception of highly authoritarian states such as China, Iran, and Cuba, most governments do not have complete control over the ICT market or internet infrastructure in their countries, meaning blocking must be implemented by multiple internet service providers (ISPs), with inconsistent results. Even in the most tightly controlled countries, tech-savvy users are able to bypass the filtering regime with circumvention tools.

In addition, the widespread adoption of HTTPS—a more secure version of the Hypertext Transfer Protocol, or HTTP—has made the blocking of specific content exceedingly difficult, and obstructing access to individual pages now often requires blocking an entire platform. For example, in July 2015, a Turkish court banned five websites for promoting the Kurdistan Workers’ Party (PKK), a designated terrorist organization. However, since the sites were hosted on WordPress—an international blog-hosting service that employs HTTPS—Turkish ISPs had to block all of WordPress, affecting more than 70 million websites. Governments are often reluctant to resort to this approach, given many services’ popularity and growing economic importance.

**Technology Companies’ Predicament**

When facing a removal request from a government, local companies have little choice but to comply, particularly if the country’s legal system offers few avenues for appeal. At the same time, some international companies have been able to satisfy governments without resorting to outright takedown, withholding unlawful content for the relevant country but leaving it online for other users around the world. In India, for example, Facebook restricted over 5,800 pieces of content in the last six months of 2014, yielding to law enforcement agencies’ requests regarding hate speech and religious criticism that ‘could cause unrest and disharmony.’

### Common Content-Removal Methods

- **Content removal requests:** Requests may come from government agencies, but also from individuals, businesses, or other entities, preferably with a court order. Depending on the company and platform, these may be subject to an internal review by the company that considers the merit of each request. In some cases, however, content is removed without much scrutiny to avoid penalties mandated by law, particularly when it is hosted within the jurisdiction that initiated the request.

- **Proactive policing by intermediaries:** Laws that hold service providers, content hosts, or webmasters disproportionately liable for third-party (user) content can motivate these intermediaries to proactively police the content on their platforms and remove anything that may result in legal penalties. This is different from purely voluntary action taken by some intermediaries to monitor their services and enforce their own policies on issues like violence or obscenity.

- **Coerced deletions:** Individual users, news sites, or other content producers can be directly pressured to delete content, for example through phone calls, arrests, and interrogations.

However, many governments go much further in shifting the burden of censorship, forcing private companies to proactively monitor their networks and err on the side of caution to comply with vaguely worded regulations. Of the 65 countries assessed in Freedom on the Net, 26 hold intermediaries liable for content to a disproportionate degree, and a number of countries increased requirements on intermediaries in the past year. In Thailand, for example, an October 2014 directive from the military junta ordered ISPs to monitor and censor content that could cause conflict or disrupt peace and order, which in practice means proactive removal of websites, comments, and videos that call for political protests or are critical of the authorities.

Such pressure forces private companies to make decisions on what is lawful and unlawful content in countries where national legislation may fail to protect legitimate speech. In efforts to expand its presence in the Chinese market, the U.S.-based professional networking site, LinkedIn, has started using a combination of human reviewers and sophisticated algorithms to restrict politically sensitive material from its users in China. On the other hand, Twitter, Facebook, and in recent years Google have been blocked in China for refusing to comply with similar requirements.

In the best cases involving censorship requests, companies act as a positive check on the repressive inten-
the human rights lawyer Walid Abulkhair refused, his prison sentence was increased from 10 to 15 years.

**Surveillance Laws and Technologies on the Rise**

Freedom on the Net research identified growing surveillance as a major trend for the third consecutive year, though the motives and impact have evolved. Undeterred by the global public backlash against the NSA practices revealed in 2013, governments in 14 of 65 countries passed new laws to increase surveillance over the past year.

**Laws Expose User Data**

Laws that require ISPs to indiscriminately retain so-called metadata—usually the time, origin, and destination of communications—or the actual content of internet traffic have been rejected by many privacy advocates, technology companies, and international bodies as a violation of the integrity, security, and privacy of communication systems. While acknowledging that these laws are often intended to assist law enforcement in investigating crimes or security threats, the UN Human Rights Committee, the Special Rapporteur for Freedom of Expression, and other entities have recognized that the requirements inherently infringe on the privacy rights of all in a manner that is disproportionate to the stated aim. Nevertheless, many countries—including democracies—have moved to retain or expand such rules.

In Australia’s Parliament passed legislation requiring telecommunications companies to store customers’ metadata for two years, allowing law enforcement and intelligence agencies to access the information without a warrant. The United Kingdom and Italy both reinstated or implemented stronger data-retention requirements in the past year, despite the fact that the European Court of Justice struck down the European Union (EU) Data Retention Directive in April 2014 as a serious breach of the fundamental right to privacy. And in the wake of terrorist attacks on the satirical magazine Charlie Hebdo and a kosher grocery in Paris, France passed sweeping legislation requiring telecommunications carriers and providers to, among other things, install “black boxes” that enable the government to collect and analyze metadata on their networks.

This trend is even more concerning in countries where internet freedom violations occur more frequently. After the Russian government issued a decree in April...
2014 requiring ISPs to update their SORM technology—the surveillance apparatus used to intercept and monitor ICT data—other former Soviet states that use the same technology followed suit. In June 2014, Kyrgyzstan instructed ISPs and mobile service providers to update their SORM technology at their own expense, store subscriber data for up to three years, and grant the authorities direct, real-time access to communications networks. Meanwhile, in Thailand, where the authorities frequently arrest or harass internet users for alleged lèse-majesté on social networks, one of many orders issued by the military government in mid-2014 mandated military surveillance and monitoring of social media sites.

Surveillance Technologies Proliferate
The adoption of problematic laws and regulations has been accompanied by the unrestricted spread of technologies that can make abuses a practical reality, particularly in countries with poor human rights records. A set of leaked files released in September 2014 from Gamma International, a surveillance and monitoring technology company, revealed information about the distribution of its FinFisher software—used to take control of targets’ computers—to governments including those of Bangladesh, Pakistan, and Bahrain. Evidence showed that the Bahraini government had obtained licenses for FinFisher to spy on the country’s most prominent lawyers, activists, and politicians.

In July 2015, a leak of documents from the information technology company Hacking Team named the governments of Azerbaijan, Egypt, Ethiopia, Uzbekistan, and Vietnam—all of which have jailed activists and bloggers—as Hacking Team clients, despite the company’s claim that it does not sell to countries where there are credible human rights concerns. At least a dozen different federal or state agencies in Mexico were also listed as having contracts with Hacking Team. Some of the agencies do not have legal or constitutional authority to engage in surveillance. In Ecuador, leaked emails provided compelling evidence that the intelligence agency targeted an opposition activist’s email account for infection with malware.

Governments Target Encryption, Anonymity
Given the mounting concerns over government surveillance, companies and internet users have taken up new tools to protect the privacy of their data and identity. In a landmark report released in May 2015, UN Special Rapporteur David Kaye underlined how encryption and anonymity are crucial to securing freedom of opinion and expression and the right to privacy, emphasizing that any restrictions must be narrowly tailored to achieve legitimate aims. Unfortunately, governments around the world have moved to limit encryption and undermine anonymity for all internet users, often citing the use of these tools by terrorists and criminals. Such restrictions disproportionately threaten the lives and work of human rights activists, journalists, opposition political figures, and members of ethnic, religious, and sexual minorities.

Stigmatizing Encryption
In the wake of revelations that intelligence agencies were collecting ordinary citizens’ communications data in bulk, technology companies have moved toward default encryption settings to enhance the privacy and security of user activity. In response, policymakers in the United Kingdom and United States have called for companies to provide intelligence agencies with a “backdoor” to user data, circumventing encryption. Authorities in China proposed a counterterrorism law in November 2014 that would require telecommunications firms to provide such government access. In Cuba, encryption services must be preapproved by the government, ensuring that none are impervious to state surveillance.

Governments around the world have moved to ban encryption and undermine anonymity for all internet users.

Many countries place limits on the scope or availability of encryption services. In India, ISPs are banned from encrypting customer data in bulk, allowing state security agencies to scan all traffic for keywords. Bahrain passed a law prohibiting the use of data encryption “for criminal intentions”; because basic forms of expression and dissent are also effectively criminalized, the new rule could be used against human rights defenders, journalists, and others.

Encryption has been stigmatized as a tool for terrorists, contributing to illegitimate arrests. In August 2015, three staff members working for Vice News were arrested in southeastern Turkey and charged with supporting terrorists after authorities found encryption software on one of their computers. Similar accusations were brought against three Al-Jazeera journalists who were detained in Egypt and the Zone 9 bloggers in Ethiopia.
Undermining Anonymity
While encryption protects the content of communications, anonymity is necessary for securing the privacy of users’ metadata. Tools such as virtual private networks (VPNs), proxies, and Tor can disguise an individual’s original internet protocol (IP) address and other details that would reveal the identity or location of users. However, governments around the globe are working to restrict these methods, undermining international norms on user anonymity. Belarus, Ethiopia, Indonesia, Iran, Kazakhstan, and Uzbekistan are among the countries that have ordered bans on Tor, or circumvention tools more broadly, and China blocked access to several popular VPNs in the past year.

Developments in Brazil reflect the complex nature of privacy online. While the country’s April 2014 Marco Civil da Internet remains a respected legal model for the protection of digital rights, the fact that anonymity is constitutionally prohibited has left the door open to new laws that could severely restrict internet freedom. During the coverage period, a court banned the now-defunct anonymous messaging application “Secret,” and legislators proposed amendments to the Marco Civil in July 2015 that would require users to register with their real name and national identification number to post on social media or blogs.

Many governments already require real-name registration for ICT access. A decree in Vietnam bans the use of pseudonyms on blogs, following the lead of increasingly strict real-name registration for social media activity in China, and all IP addresses in Iran must be registered with the authorities.

Arrests and Intimidation of Users Escalate
*Freedom on the Net* has previously noted an increase in offline punishments for online expression, but the penalties and reprisals reached a new level of severity in the past year, as both authorities and criminal groups made public examples of internet users who opposed their agenda.

Prison Sentences
Of the 65 countries reviewed, 40 imprisoned people for sharing political or social content through digital networks, up from 38 in last year’s report. Courts in seven countries imposed or upheld prison sentences of seven years or more. Sentences issued during 2015 for alleged online insults to Thailand’s monarchy have exceeded 25 years in prison. In 2015, a Cairo court handed life sentences to two journalists for online coverage of the bloody crackdown on a Muslim Brotherhood protest. In September 2014, a court in China sentenced Uighur academic Ilham Tohti, a renowned moderate, to life imprisonment, partly for running a website on Uighur affairs.

China was not the only country to target vulnerable minorities. Eight men were jailed in Egypt in December 2014 for appearing in a video documenting a gay couple’s wedding ceremony. A court sentenced them to three years’ imprisonment for “inciting debauchery,” later reduced to one year.

Violence and Harassment
In addition to formal prosecutions, internet users faced physical violence and intimidation in a variety of forms. The web itself has sometimes been used to publicize such attacks and amplify the deterrent effect on other users. In Syria, IS militants posted videos showing the executions of international journalists, including Kenji Goto, a veteran Japanese reporter who founded the website *Independent Press* to cover humanitarian issues in 1996. Assaults in the Mexican border state of Tamaulipas murdered Maria del Rosario Fuentes Rubio for administering a Twitter and Facebook network that reported criminal violence, then broadcast photos of her body using her mobile phone and Twitter account.

Even when threats precede attacks, targeted individuals do not always receive the appropriate protection. Four bloggers in Bangladesh were fatally stabbed in separate incidents over the course of seven months in 2015, despite the fact that Islamist extremists had openly threatened their lives for expressing secular viewpoints.

Many online journalists and activists fled their home countries, though some found no safety abroad. Blogger Assad Hanna left Syria following online threats stemming from his criticism of the regime, but he was badly injured by knife-wielding assailants at his apartment in Turkey.

Other users were targeted for online activism promoting women’s rights, or in ways that seemed motivated by their gender. In February 2015, Indian activist Sunitha Krishnan launched a “Shame the Rapist” campaign that featured a video demonstrating how to blur the faces of victims in footage of assaults shared on the messaging platform WhatsApp. Her car was stoned just hours after the campaign began. In January 2015, unknown individuals hacked a social network account belonging to Larysa Shchyrakova, a Belarus-based independent journalist and civic activ-
They posted explicit photos of Shchyrakova that were apparently taken from a computer confiscated by the state security service in 2010.

**Youth Targeted**

Internet users tend to be younger than the general population on average, and police in several countries sought out teenagers who offended national leaders on social media in the past year. In western Turkey, police visited a classroom to question a 13-year-old on suspicion of “insulting” President Recep Tayyip Erdoğan on Facebook. An 18-year-old was among six people arrested in Venezuela for tweeting about the death of a national lawmaker. Police in Belarus threatened to fine student Dmitry Dayneko after an opposition website shared his YouTube video calling on President Alyaksandr Lukashenka to take the “ice bucket challenge,” whose participants—including several international politicians—sought charitable sponsorships for publicly drenching themselves in cold water.

In one particularly egregious case, 16-year-old Singaporean blogger Amos Yee was charged under a new law designed to combat online harassment after he celebrated the death of the country’s founding prime minister, Lee Kuan Yew, on video. Yee was acquitted on that charge but sentenced for obscenity and wounding religious feeling, spending four weeks in jail. The attention drawn by the prosecution fueled anger among Lee’s supporters, and Yee was assaulted outside the courtroom. In the words of his follow-up video: “All that from a video taken by a boy in his room, with a camera, in his pajamas.”

Iranian cartoonist Atena Farghadani was sentenced to 12 years in prison on charges of insulting state officials and spreading propaganda for posting this image on Facebook depicting members of parliament as animals, casting votes on proposed legislation to limit reproductive rights.
Emerging Issues

Over the past year, several decisions by legal or regulatory bodies generated significant global discussion on how to guarantee access to information while respecting other rights. The fight for “net neutrality” protections in the United States reinforced efforts in other countries to secure open and nondiscriminatory access to online content. Meanwhile, in the EU, a decision regarding search engines’ responsibility for personal data bolstered the concept of the “right to be forgotten,” which was then taken up by several national legislatures.

Net Neutrality

Net neutrality refers to the principle that all internet traffic should be treated equally by network owners, and not obstructed or accelerated based on its type or the identity of senders and recipients. This ensures that all internet users have equal access to the widest array of content and platforms available, while preventing dominant companies from skewing the online sphere in their favor. For example, the principle prevents major telecommunications firms from blocking Voice over IP (VoIP) services that may compete with their traditional telephone services. It also means that users do not need to suffer lower speeds imposed for high-bandwidth content like streaming video, which can serve as an important news source—especially in settings where traditional media are constrained or inadequate.

Some regulatory agencies have recently intervened to uphold net neutrality. In the United States, after more than a year of significant public debate and unprecedented levels of citizen feedback, the Federal Communications Commission approved new rules that allow it to regulate the internet as a public utility, including strong provisions that limit the extent to which ISPs can pick and choose the content that reaches their subscribers.

Similarly in Canada, the telecommunications regulator issued a ruling in January 2015 stating that companies cannot set rules or prices that favor their streaming services over those of competitors, after it was revealed that Bell had been exempting its mobile application from the download limits that it places on competitors’ apps. Other countries, such as Iceland and Argentina, passed resolutions guaranteeing the principle of net neutrality.

Meanwhile, a number of governments moved in the opposite direction. In Russia, the Federal Anti-Monopoly Service put forth a proposal in October 2014 that would allow some companies to pay for prioritized content delivery, and included references to data-heavy platforms like Skype and YouTube. In India, service providers took steps in 2014 to limit access to communication tools—such as VoIP services—that threatened their profits. They were supported by the Telecom Regulatory Authority, which created a draft regulatory framework allowing extra fees for consumers using communication apps. Indian users responded in large numbers, with more than a million people submitting comments to the regulatory authority; the issue is now under parliamentary review.

Complicating this debate is the practice of “zero rating,” in which private companies offer subscribers free access to certain popular online platforms in order to attract new users. Proponents of these programs argue that they could significantly increase access to useful web applications, but critics warn that they could result in a stratified system, with those who cannot afford full access relegated to a lesser version of the internet. Internet.org (later renamed “Free Basics”), Facebook’s initiative to offer affordable access to select platforms and applications, was rolled out in several countries across Asia, sub-Saharan Africa, and Latin America. In Brazil, plans to introduce Internet.org triggered discussion on whether zero rating is legal under the Marco Civil da Internet’s net neutrality provisions. In India and Indonesia, some service providers opted out of the Facebook program, citing both business and net neutrality concerns.

The ‘Right to Be Forgotten’

In May 2014, the Court of Justice of the European Union granted individuals the right to request that search engines hide links to public information about them if it is no longer accurate or relevant, establishing their “right to be forgotten.” However, aside from information about public figures, the ruling provided little guidance as to what types of information should
be hidden or retained in the public interest, meaning search engines would have to decide on a case-by-case basis, in an internal process that lacks the oversight and transparency of established legal proceedings.

For example, in Germany, Google complied with requests to delink news content about a sexual assault that named the victim, though the articles remained on the internet and still appeared in search results outside the country. In Hungary, meanwhile, Google did not comply with a request from an official who wanted to suppress information about a past criminal conviction. Some privacy advocates fought to extend the right to be forgotten beyond national borders. In June 2015, the French data protection agency demanded that Google carry out removals across all of its sites, meaning the search results would be omitted even for users outside France.

Signaling the development of a global trend, at least six non-EU countries, including Argentina, Colombia, Japan, Kenya, Mexico, and Russia, considered an individual’s right to be forgotten during the coverage period. A Colombian court struck a balance of sorts in a case involving a newspaper article that implicated an individual in a criminal matter. Although the court protected Google from liability and did not order the search engine to remove links, the newspaper was required to publish an update reflecting the verdict, and make the content less likely to appear in search results by manipulating the tags that describe a page’s content for public indexing. It is unclear whether the ruling will affect other media, but it could burden news outlets or inadvertently make content on related topics less accessible.

The greatest gains have been made through legislative changes or judicial decisions.

Two other examples were particularly problematic. In September 2014, businessman Carlos Sánchez de la Peña asked Mexico’s independent privacy agency to order Google Mexico to remove three results that linked to content alleging his involvement in corruption—information that digital rights groups argued was in the public interest. The agency threatened the company with sanctions after it refused to comply. And in July 2015, Russian president Vladimir Putin signed legislation allowing individuals to request that search engines remove links to certain information within 10 days. Unlike in the European decision, this legislation also allows public figures to make such requests, setting the stage for the possible censorship of information in the public interest.

Conclusion

In many ways, the past year was one of consolidation and adaptation of internet restrictions rather than dramatic new declines. Governments that had already greatly expanded their arsenal of tools for controlling the online sphere—by disrupting ICT networks, blocking and filtering content, and conducting invasive surveillance—are now strengthening their application of these methods. As blocking has become less effective, more governments have shifted to censoring content through removal requests or more forceful, coercive tactics. And as savvy internet users increasingly turn to encryption and anonymity tools to protect their rights, government officials across the political spectrum are seeking to undermine these obstacles to surveillance, potentially making the internet less secure for everyone.

It remains to be seen whether repressive efforts will be sustainable in the long run. The global struggle for internet freedom led to several positive achievements over the past year, raising the possibility of greater advances in the future. Digital activism has been and remains a vital driver of change around the world, particularly in societies that lack political rights and press freedom. The greatest gains, however, have been made through legislative changes or judicial decisions, indicating that countries with meaningful political debates and independent judiciaries have a distinct advantage in safeguarding internet freedom over their more authoritarian counterparts. These victories and others like them could help ensure that the fight for a free and open internet ultimately succeeds, despite the setbacks that have affected so much of the world in recent years.
The 65 countries covered in *Freedom on the Net* represent 88 percent of the world’s internet user population. Over 40 percent of global internet users live in three countries — China, the United States, or India — that span the spectrum of internet freedom environments, from Free to Not Free.
GLOBAL INTERNET USERS

Over 3 billion people have access to the internet.

According to Freedom House estimates:

61% live in countries where criticism of the government, military, or ruling family has been subject to censorship.

47% live in countries where individuals were attacked or killed for their online activities since June 2014.

58% live in countries where bloggers or ICT users were jailed for sharing content on political, social, and religious issues.

47% live in countries where corruption allegations against top government or business figures can be repressed or punished.

45% live in countries where posting satirical writings, videos, or cartoons can result in censorship or jail time.

34% live in countries where LGBTI voices have been silenced or where access to resources has been limited by authorities.

38% live in countries where popular social media or messaging apps were blocked in the past year.

34% live under governments which disconnected internet or mobile phone access in 2014-2015, often for political reasons.
## KEY INTERNET CONTROLS BY COUNTRY

<table>
<thead>
<tr>
<th>Country (by FOTN 2015 ranking)</th>
<th>FOTN 2015 score (0=Most Free, 100=Least Free)</th>
<th>FOTN 2015 Status (F=Free, PR=Partly Free, NF=Not Free)</th>
<th>Social media and/or communications apps blocked</th>
<th>Political, social, and/or religious content blocked</th>
<th>Localized or nationwide ICT shut down</th>
<th>Pro-government commentators manipulate online discussions</th>
<th>New laws/directives increasing censorship or punishment passed</th>
<th>New laws/directives increasing surveillance or restricting anonymity passed</th>
<th>Online journalist/blogger/ICT user arrested, imprisoned, and/or in prolonged detention for political or social content</th>
<th>Online journalist/blogger/ICT user physically attacked or killed (including while in custody)</th>
<th>Technical attacks against government critics and human rights organizations</th>
<th>TOTAL # of Key Internet Controls employed in 2014-2015, by country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iceland</td>
<td>6</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estonia</td>
<td>7</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td>16</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>18</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td>19</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td>19</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>22</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td>23</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>24</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Georgia</td>
<td>24</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td>24</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>24</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td>27</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phillipines</td>
<td>27</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>South Africa</td>
<td>27</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Armenia</td>
<td>28</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td>29</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kenya</td>
<td>29</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Colombia</td>
<td>32</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nigeria</td>
<td>33</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>South Korea</td>
<td>34</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>35</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uganda</td>
<td>36</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ecuador</td>
<td>37</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ukraine</td>
<td>37</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunisia</td>
<td>38</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Angola</td>
<td>39</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td>39</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>India</td>
<td>40</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malawi</td>
<td>40</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zambia</td>
<td>40</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td>41</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indonesia</td>
<td>42</td>
<td>PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Internet control observed during the June 2014 - May 2015 coverage period.
- Internet control observed after May 31, 2014 until the time of writing.
- ICT user arrested prior to coverage period but serving part or all of prison sentence during coverage period.
### Country (by FOTN 2015 ranking)

<table>
<thead>
<tr>
<th>Country</th>
<th>FOTN Score</th>
<th>FOTN Status</th>
<th>Social media and/or communications apps blocked</th>
<th>Political, social, and/or religious content blocked</th>
<th>Localized or nationwide ICT shut down</th>
<th>Progovernment commentators manipulate online discussions</th>
<th>New law/directive increasing censorship or punishment passed</th>
<th>New law/directive increasing surveillance or restricting anonymity passed</th>
<th>Online journalist/blogger/ICT user arrested, imprisoned and/or in prolonged detention for political or social content</th>
<th>Online journalist/blogger/ICT user physically attacked or killed (including while in custody)</th>
<th>Technical attacks against government critics and human rights organizations</th>
<th>TOTAL # of Key Internet Controls employed in 2014-2015, by country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malaysia</td>
<td>43</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4</td>
</tr>
<tr>
<td>Morocco</td>
<td>43</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>3</td>
</tr>
<tr>
<td>Lebanon</td>
<td>45</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>3</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>47</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>1</td>
</tr>
<tr>
<td>Cambodia</td>
<td>48</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>1</td>
</tr>
<tr>
<td>Jordan</td>
<td>50</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>2</td>
</tr>
<tr>
<td>Rwanda</td>
<td>50</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>1</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>51</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4</td>
</tr>
<tr>
<td>Libya</td>
<td>54</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>3</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>56</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>56</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4</td>
</tr>
<tr>
<td>Venezuela</td>
<td>57</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4</td>
</tr>
<tr>
<td>Turkey</td>
<td>58</td>
<td>PF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>7</td>
</tr>
<tr>
<td>Egypt</td>
<td>61</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>5</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>61</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>7</td>
</tr>
<tr>
<td>Russia</td>
<td>62</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>6</td>
</tr>
<tr>
<td>Myanmar</td>
<td>63</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>6</td>
</tr>
<tr>
<td>Thailand</td>
<td>63</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4</td>
</tr>
<tr>
<td>Belarus</td>
<td>64</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>6</td>
</tr>
<tr>
<td>The Gambia</td>
<td>65</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>6</td>
</tr>
<tr>
<td>Sudan</td>
<td>65</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>3</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>68</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4</td>
</tr>
<tr>
<td>Pakistan</td>
<td>69</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>6</td>
</tr>
<tr>
<td>Bahrain</td>
<td>72</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>6</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>73</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>6</td>
</tr>
<tr>
<td>Vietnam</td>
<td>76</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>6</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>78</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>6</td>
</tr>
<tr>
<td>Cuba</td>
<td>81</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>5</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>82</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>5</td>
</tr>
<tr>
<td>Iran</td>
<td>87</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>5</td>
</tr>
<tr>
<td>Syria</td>
<td>87</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>7</td>
</tr>
<tr>
<td>China</td>
<td>88</td>
<td>NF</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>9</td>
</tr>
</tbody>
</table>

- ● = Internet control observed during the June 2014 - May 2015 coverage period.
- ● = Internet control observed after May 31, 2014 until the time of writing.
- ● = ICT user arrested prior to coverage period but serving part or all of prison sentence during coverage period.

www.freedomhouse.org
Freedom on the Net 2015 assessed 65 countries around the globe. The project is expected to expand to more countries in the future.
Freedom on the Net measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of FREE (0-30 points), PARTLY FREE (31-60 points), or NOT FREE (61-100 points).

Ratings are determined through an examination of three broad categories:

A. OBSTACLES TO ACCESS: Assesses infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; and legal, regulatory, and ownership control over internet and mobile phone access providers.

B. LIMITS ON CONTENT: Examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.

C. VIOLATIONS OF USER RIGHTS: Measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.
Freedom on the Net 2015 covers 65 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

0 = Most Free
100 = Least Free

**Asia**
- Japan 22
- Philippines 27
- South Korea 34
- India 40
- Singapore 41
- Indonesia 42
- Malaysia 43
- Sri Lanka 47
- Cambodia 48
- Bangladesh 51
- Myanmar 63
- Thailand 63
- Pakistan 69
- Vietnam 76
- China 88

**Sub-Saharan Africa**
- South Africa 27
- Kenya 29
- Nigeria 33
- Uganda 36
- Angola 39
- Malawi 40
- Zambia 40
- Rwanda 50
- Zimbabwe 56
- Sudan 65
- The Gambia 65
- Ethiopia 82

**Australia, Canada, European Union, Iceland & United States**
- Iceland 6
- Estonia 7
- Canada 16
- Germany 18
- Australia 19
- United States 19
- Italy 23
- France 24
- Hungary 24
- United Kingdom 24
INTERNET FREEDOM VS. PRESS FREEDOM

In the majority of the 65 countries assessed, the country’s digital media environment was more free than its traditional media sphere. This difference is evident from the comparison between a country’s score on Freedom House’s Freedom on the Net 2015 (represented as the bar graph) and Freedom of the Press 2015 (represented as the scatterplot, ▲) surveys, the latter of which measures media freedom in the broadcast, radio, and print domains.

The figure above shows the 43 countries in this edition with a score difference of 10 points or greater. While pressures that constrain expression in print or broadcast media have the potential to inhibit the online sphere, our data shows that the number of countries with a significantly more free internet environment increased from 37 countries in the last edition, indicating that the internet may be proving more resilient to government control. Nevertheless, attempts by governments to rein in online freedoms remain a cause for concern, particularly in countries that lack press freedom where the internet is often the last remaining outlet for free expression and independent news.
The figure above depicts the relationship between internet freedom, internet access, and economic activity as measured by gross domestic product (GDP) per capita data. The x-axis considers a country’s score in the 2015 edition of Freedom on the Net, adjusted to exclude aspects related to internet access. Levels of internet penetration are plotted against the y-axis, using 2014 statistics from the United Nations International Telecommunication Union (ITU). Finally, the size of each plot is indicative of its GDP per capita (at purchasing power parity, PPP), according to the latest figures from the World Bank.

While wealth generally translates to greater access, neither are a decisive indicator of free expression, privacy, or access to information online, as evidenced by the range of internet freedom environments represented at the top of the chart. The Gulf countries lead a cluster of rentier economies investing in high-tech tools to restrict online freedoms. Meanwhile, as “partly free” countries in sub-Saharan Africa and Southeast Asia continue to develop, they would be wise to consider a free and open internet as a mechanism for a prosperous, diversified economy.
### Overview of Score Changes

<table>
<thead>
<tr>
<th>Country</th>
<th>FOTN 2014</th>
<th>FOTN 2015</th>
<th>Overall Trajectory</th>
<th>FOTN 2015 Status</th>
<th>A. Obstacles to Access</th>
<th>B. Limits on Content</th>
<th>C. Violations of User Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bangladesh</td>
<td>49</td>
<td>51</td>
<td>▼</td>
<td>Partly Free</td>
<td>12</td>
<td>12</td>
<td>27</td>
</tr>
<tr>
<td>Cambodia</td>
<td>47</td>
<td>48</td>
<td>▼</td>
<td>Partly Free</td>
<td>14</td>
<td>15</td>
<td>19</td>
</tr>
<tr>
<td>China</td>
<td>87</td>
<td>88</td>
<td>▼</td>
<td>Not Free</td>
<td>18 ▲</td>
<td>30 ▼ ▲</td>
<td>40 ▲</td>
</tr>
<tr>
<td>India</td>
<td>42</td>
<td>40</td>
<td>▲</td>
<td>Partly Free</td>
<td>12 ▲ ▲</td>
<td>10 ▲ ▲</td>
<td>18 ▲ ▲</td>
</tr>
<tr>
<td>Indonesia</td>
<td>42</td>
<td>42</td>
<td>▼</td>
<td>Partly Free</td>
<td>11</td>
<td>12</td>
<td>19</td>
</tr>
<tr>
<td>Japan</td>
<td>22</td>
<td>22</td>
<td></td>
<td>Free</td>
<td>4</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>Malaysia</td>
<td>42</td>
<td>43</td>
<td>▼</td>
<td>Partly Free</td>
<td>8</td>
<td>14</td>
<td>21</td>
</tr>
<tr>
<td>Myanmar</td>
<td>60</td>
<td>63</td>
<td>▼</td>
<td>Not Free</td>
<td>18 ▲ ▲ ▲</td>
<td>17 ▲ ▲ ▲</td>
<td>28 ▲ ▲ ▲</td>
</tr>
<tr>
<td>Pakistan</td>
<td>69</td>
<td>69</td>
<td></td>
<td>Not Free</td>
<td>20</td>
<td>20</td>
<td>29</td>
</tr>
<tr>
<td>Philippines</td>
<td>27</td>
<td>27</td>
<td></td>
<td>Free</td>
<td>10</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>Singapore</td>
<td>40</td>
<td>41</td>
<td>▼</td>
<td>Partly Free</td>
<td>6</td>
<td>14</td>
<td>21</td>
</tr>
<tr>
<td>South Korea</td>
<td>33</td>
<td>34</td>
<td>▼</td>
<td>Partly Free</td>
<td>3</td>
<td>14</td>
<td>17</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>58</td>
<td>47</td>
<td>▲</td>
<td>Partly Free</td>
<td>14 ▲ ▲ ▲ ▲</td>
<td>13 ▲ ▲ ▲ ▲</td>
<td>20 ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Thailand</td>
<td>62</td>
<td>63</td>
<td>▼</td>
<td>Not Free</td>
<td>9 ▲ ▲ ▲ ▲ ▲</td>
<td>22 ▲ ▲ ▲ ▲ ▲</td>
<td>32 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Vietnam</td>
<td>76</td>
<td>76</td>
<td></td>
<td>Not Free</td>
<td>13 ▲ ▲ ▲ ▲ ▲</td>
<td>29 ▲ ▲ ▲ ▲ ▲</td>
<td>34 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
</tbody>
</table>

#### Eurasia

<table>
<thead>
<tr>
<th>Country</th>
<th>FOTN 2014</th>
<th>FOTN 2015</th>
<th>Overall Trajectory</th>
<th>FOTN 2015 Status</th>
<th>A. Obstacles to Access</th>
<th>B. Limits on Content</th>
<th>C. Violations of User Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Armenia</td>
<td>28</td>
<td>28</td>
<td></td>
<td>Free</td>
<td>6 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>10 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>12 ▲ ▲ ▲ ▲ ▲ ▲ ^</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>55</td>
<td>56</td>
<td>▼</td>
<td>Partly Free</td>
<td>13 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>19 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>24 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Belarus</td>
<td>62</td>
<td>64</td>
<td>▼</td>
<td>Not Free</td>
<td>15 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>21 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>28 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Georgia</td>
<td>26</td>
<td>24</td>
<td>▲</td>
<td>Free</td>
<td>7 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>6 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>11 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>60</td>
<td>61</td>
<td>▼</td>
<td>Not Free</td>
<td>14 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>23 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>24 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>34</td>
<td>35</td>
<td>▼</td>
<td>Partly Free</td>
<td>11 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>8 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>16 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Russia</td>
<td>60</td>
<td>62</td>
<td>▼</td>
<td>Not Free</td>
<td>10 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>23 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>29 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Turkey</td>
<td>55</td>
<td>58</td>
<td>▼</td>
<td>Partly Free</td>
<td>13 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>20 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>25 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Ukraine</td>
<td>33</td>
<td>37</td>
<td>▼</td>
<td>Partly Free</td>
<td>8 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>10 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>19 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>79</td>
<td>78</td>
<td>▲</td>
<td>Not Free</td>
<td>19 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>28 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>31 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
</tbody>
</table>

#### Latin America

<table>
<thead>
<tr>
<th>Country</th>
<th>FOTN 2014</th>
<th>FOTN 2015</th>
<th>Overall Trajectory</th>
<th>FOTN 2015 Status</th>
<th>A. Obstacles to Access</th>
<th>B. Limits on Content</th>
<th>C. Violations of User Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td>27</td>
<td>27</td>
<td></td>
<td>Free</td>
<td>7 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>8 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>12 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Brazil</td>
<td>30</td>
<td>29</td>
<td>▲</td>
<td>Free</td>
<td>7 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>6 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>16 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Colombia</td>
<td>30</td>
<td>32</td>
<td>▼</td>
<td>Partly Free</td>
<td>8 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>8 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>16 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Cuba</td>
<td>84</td>
<td>81</td>
<td>▲</td>
<td>Not Free</td>
<td>22 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>27 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>32 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Ecuador</td>
<td>37</td>
<td>37</td>
<td></td>
<td>Partly Free</td>
<td>8 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>11 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>18 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Mexico</td>
<td>39</td>
<td>39</td>
<td></td>
<td>Partly Free</td>
<td>9 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>10 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>20 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td>Venezuela</td>
<td>56</td>
<td>57</td>
<td>▼</td>
<td>Partly Free</td>
<td>17 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>18 ▲ ▲ ▲ ▲ ▲ ▲</td>
<td>22 ▲ ▲ ▲ ▲ ▲ ▲</td>
</tr>
</tbody>
</table>

A Freedom on the Net score increase represents a negative trajectory (▼) for internet freedom, while a score decrease represents a positive trajectory (▲) for internet freedom.

▼ = Decline  ▲ = Improvement  Blank = No Change
Overall Category Trajectories

<table>
<thead>
<tr>
<th>Country</th>
<th>FOTN 2014</th>
<th>FOTN 2015</th>
<th>Overall Trajectory</th>
<th>FOTN 2015 Status</th>
<th>A. Obstacles to Access</th>
<th>B. Limits on Content</th>
<th>C. Violations of User Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Middle East &amp; North Africa</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bahrain</td>
<td>74</td>
<td>72</td>
<td>▲</td>
<td>Not Free</td>
<td>11</td>
<td>▲</td>
<td>27</td>
</tr>
<tr>
<td>Egypt</td>
<td>60</td>
<td>61</td>
<td>▼</td>
<td>Not Free</td>
<td>14</td>
<td>▲</td>
<td>13</td>
</tr>
<tr>
<td>Iran</td>
<td>89</td>
<td>87</td>
<td>▲</td>
<td>Not Free</td>
<td>20</td>
<td>▲</td>
<td>31</td>
</tr>
<tr>
<td>Jordan</td>
<td>48</td>
<td>50</td>
<td>▲</td>
<td>Partly Free</td>
<td>12</td>
<td>▲</td>
<td>16</td>
</tr>
<tr>
<td>Lebanon</td>
<td>47</td>
<td>45</td>
<td>▲</td>
<td>Partly Free</td>
<td>13</td>
<td>▲</td>
<td>12</td>
</tr>
<tr>
<td>Libya</td>
<td>48</td>
<td>54</td>
<td>▼</td>
<td>Partly Free</td>
<td>20</td>
<td>▼</td>
<td>12</td>
</tr>
<tr>
<td>Morocco</td>
<td>44</td>
<td>43</td>
<td>▲</td>
<td>Partly Free</td>
<td>11</td>
<td>▲</td>
<td>9</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>73</td>
<td>73</td>
<td>Not Free</td>
<td>15</td>
<td>24</td>
<td>13</td>
<td>22</td>
</tr>
<tr>
<td>Syria</td>
<td>88</td>
<td>87</td>
<td>Not Free</td>
<td>24</td>
<td>26</td>
<td>12</td>
<td>34</td>
</tr>
<tr>
<td>Tunisia</td>
<td>39</td>
<td>38</td>
<td>▲</td>
<td>Partly Free</td>
<td>10</td>
<td>▲</td>
<td>8</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>67</td>
<td>68</td>
<td>▼</td>
<td>Not Free</td>
<td>14</td>
<td>▲</td>
<td>22</td>
</tr>
<tr>
<td><strong>Sub-Saharan Africa</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Angola</td>
<td>38</td>
<td>39</td>
<td>▼</td>
<td>Partly Free</td>
<td>14</td>
<td>▲</td>
<td>8</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>80</td>
<td>82</td>
<td>▼</td>
<td>Not Free</td>
<td>23</td>
<td>▲</td>
<td>28</td>
</tr>
<tr>
<td>Kenya</td>
<td>28</td>
<td>29</td>
<td>▼</td>
<td>Free</td>
<td>9</td>
<td>▲</td>
<td>7</td>
</tr>
<tr>
<td>Malawi</td>
<td>42</td>
<td>40</td>
<td>▲</td>
<td>Partly Free</td>
<td>15</td>
<td>▲</td>
<td>12</td>
</tr>
<tr>
<td>Nigeria</td>
<td>33</td>
<td>33</td>
<td>▲</td>
<td>Partly Free</td>
<td>10</td>
<td>▲</td>
<td>8</td>
</tr>
<tr>
<td>Rwanda</td>
<td>50</td>
<td>50</td>
<td>▲</td>
<td>Partly Free</td>
<td>11</td>
<td>▲</td>
<td>20</td>
</tr>
<tr>
<td>South Africa</td>
<td>26</td>
<td>27</td>
<td>▼</td>
<td>Free</td>
<td>8</td>
<td>▲</td>
<td>8</td>
</tr>
<tr>
<td>Sudan</td>
<td>65</td>
<td>65</td>
<td>Not Free</td>
<td>18</td>
<td>19</td>
<td>▲</td>
<td>28</td>
</tr>
<tr>
<td>The Gambia</td>
<td>65</td>
<td>65</td>
<td>Not Free</td>
<td>18</td>
<td>▲</td>
<td>21</td>
<td>26</td>
</tr>
<tr>
<td>Uganda</td>
<td>34</td>
<td>36</td>
<td>▼</td>
<td>Partly Free</td>
<td>11</td>
<td>▲</td>
<td>7</td>
</tr>
<tr>
<td>Zambia</td>
<td>43</td>
<td>40</td>
<td>▲</td>
<td>Partly Free</td>
<td>11</td>
<td>▲</td>
<td>12</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>55</td>
<td>56</td>
<td>▼</td>
<td>Partly Free</td>
<td>15</td>
<td>▲</td>
<td>16</td>
</tr>
<tr>
<td><strong>Australia, Canada, European Union, Iceland &amp; United States</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td>17</td>
<td>19</td>
<td>▼</td>
<td>Free</td>
<td>2</td>
<td>▲</td>
<td>5</td>
</tr>
<tr>
<td>Canada</td>
<td>15</td>
<td>16</td>
<td>▼</td>
<td>Free</td>
<td>3</td>
<td>▲</td>
<td>4</td>
</tr>
<tr>
<td>Estonia</td>
<td>8</td>
<td>7</td>
<td>▲</td>
<td>Free</td>
<td>1</td>
<td>▲</td>
<td>3</td>
</tr>
<tr>
<td>France</td>
<td>20</td>
<td>24</td>
<td>▼</td>
<td>Free</td>
<td>3</td>
<td>▲</td>
<td>6</td>
</tr>
<tr>
<td>Germany</td>
<td>17</td>
<td>18</td>
<td>▼</td>
<td>Free</td>
<td>4</td>
<td>▲</td>
<td>5</td>
</tr>
<tr>
<td>Hungary</td>
<td>24</td>
<td>24</td>
<td>▼</td>
<td>Free</td>
<td>4</td>
<td>▲</td>
<td>9</td>
</tr>
<tr>
<td>Iceland</td>
<td>6</td>
<td>6</td>
<td>▼</td>
<td>Free</td>
<td>1</td>
<td>▲</td>
<td>1</td>
</tr>
<tr>
<td>Italy</td>
<td>22</td>
<td>23</td>
<td>▼</td>
<td>Free</td>
<td>4</td>
<td>▲</td>
<td>6</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>24</td>
<td>24</td>
<td>▼</td>
<td>Free</td>
<td>2</td>
<td>▲</td>
<td>6</td>
</tr>
<tr>
<td>United States</td>
<td>19</td>
<td>19</td>
<td>▼</td>
<td>Free</td>
<td>3</td>
<td>▲</td>
<td>2</td>
</tr>
</tbody>
</table>

A *Freedom on the Net* score increase represents a negative trajectory (▼) for internet freedom, while a score decrease represents a positive trajectory (▲) for internet freedom.

▼ = Decline ▲ = Improvement Blank = No Change
Angola

Key Developments: June 2014 – May 2015

- In May 2015, defamation charges against investigative journalist and blogger Rafael Marques de Morais culminated in a guilty verdict, which carried a six-month suspended prison sentence and an order to remove all copies and references of the offending material from the country and the internet (see Content Removal and Prosecutions and Detentions for Online Activities).

- Throughout 2014, members of a Facebook group called Central Angola 7311 organized via text message a series of flash mob demonstrations at government ministries to protest restrictions on freedom of expression and assembly (see Digital Activism).

- The authorities increasingly targeted critical comments posted on social media platforms, arresting one user for a Facebook post in April 2015 (see Prosecutions and Detentions for Online Activities).

- In June 2015, leaked emails from the surveillance company Hacking Team revealed efforts by Angola’s intelligence agency to acquire Hacking Team’s notorious Remote Control System (RCS) sometime in 2013 (see Surveillance, Privacy, and Anonymity).

- The critical news blog Maka Angola was attacked and taken down for several days at a time in the lead-up to the criminal defamation case against the outlet’s owner, Rafael Marques de Morais (see Technical Violence).
Introduction

Angola boasts one of the largest mobile telecommunications markets in sub-Saharan Africa as a result of heavy government investments to improve access to information and communication technologies (ICTs) since 2005, leading to a steady increase in internet access via mobile devices, mainly in urban areas. Nonetheless, extreme income inequality, high costs, and poor infrastructure outside of major cities are major obstacles to ICT access for poorer Angolans who mostly live in rural areas.

Despite progress in ICT development, the telecom sector is effectively under state control, with high ranking government officials owning large shares of the major telecommunications service providers. Further, the president has legal powers to control and punish internet service providers (ISPs) for unspecified offenses under the 2011 Law on Electronic Communications and Information Company Services.

Political rights and civil liberties are tightly restricted by the ruling party under President José Eduardo dos Santos, who has been in power for over 35 years. While the government did not block access to online content or communication applications during the coverage period, the government seemed increasingly intent on cracking down against online dissent through legal and extralegal means. In April 2015, one Facebook user was arrested for a post that had recounted the user’s abuse at the hands of a military general. He was held in a military prison without charges and released a week later only after he agreed to take down the offending post. In May 2015, ongoing defamation charges against investigative journalist and blogger Rafael Marques de Morais culminated in a guilty conviction, which carried a six-month suspended prison sentence and an impossible order to remove all copies and references of the investigative expose on the internet. In the lead-up to his court case, de Morais’s critical news blog *Maka Angola* was attacked and taken down for several days at a time.

Meanwhile, surveillance of online communications remained a concern, particularly following leaked emails from the surveillance company Hacking Team, which revealed efforts by Angola’s intelligence agency to acquire Hacking Team’s notorious Remote Control System (RCS) sometime in 2013.

Obstacles to Access

*Internet and mobile phone penetration increased incrementally from 2013 to 2014, hindered largely by high costs and poor infrastructure that limit access primarily in urban areas. Senior government officials have direct and indirect shareholder participation in many Angolan ICT companies, providing the government with some level of control over the sector, while the 2011 Law on Electronic Communications empowers the president to control the ICT sector at will.*

Availability and Ease of Access

Access to ICTs in Angola has improved markedly with increasing investments in the telecommunications sector since the end of the country’s decades-long civil war in 2002. In 2014, internet use in Angola reached a penetration rate of 21 percent, up from 19 percent in 2013, according to the latest available data from the International Telecommunications Union (ITU). Access to mobile phones

---

Angola

is much higher with a penetration rate of over 63 percent in 2014, slightly up from 62 percent in 2013, and over 12 percent of Angolans have mobile broadband subscriptions. Meanwhile, fixed-line broadband subscriptions remain very low with a penetration rate of only 0.4 percent in 2014 and are largely concentrated in the capital city, Luanda, due to the country’s high poverty rate and poor infrastructure in rural areas.

High costs are the main hindrance to increasing ICT access for the majority of Angolans whose median annual per capita income was US$720. For those able to access the internet in urban areas, subscriptions start at US$50 per month but can cost as high as US$100 per month for connections via satellite or WiMax. Unlimited internet subscriptions cost an average of US$150 per month, while USB dongle devices that provide wireless access cost between US$50 and $60. Consequently, less than 8 percent of Angolan households have internet access at home. Mobile internet packages come at a monthly cost of about US$45, while internet cafes charge approximately US$1 for 30 minutes. Due to these high prices, most internet users in Luanda go online at their workplaces.

In rural areas, voice and data services can be twice as expensive and of much poorer quality, subject to frequent cuts and extremely slow connection speeds as a result of poor infrastructure. According to the latest data from Akamai’s “State of the Internet” report, average broadband connection speed in Angola is 2.0 Mbps (compared to a global average of 3.9 Mbps). ICT access is further hindered by the country’s fractured electricity system that serves less than 40 percent of the population, mostly in urban areas.

Restrictions on Connectivity

There were no restrictions on connectivity to internet or mobile phone networks reported during the coverage period.

Angola’s domestic backbone is currently comprised of microwave, VSAT, and fiber-optic cables. Connection to the international internet goes through the West Africa Cable System (WACS) and South Atlantic 3 (SAT-3) cable, the latter of which is operated by the state-owned Angola Telecom, which may enable the government to partially control internet connectivity if desired.

In 2014, Angola began construction on the South Atlantic Cable System (SACS), a submarine fiber-optic cable connecting Brazil and Angola that aims to reduce the bandwidth costs associated with the distance that internet traffic currently has to travel from Europe and the United States. Construction of SACS is expected to be completed by late 2016.

---

ICT Market

Senior government officials have direct and indirect shareholder participation in many Angolan companies, including ISPs and mobile phone providers, providing the government with some level of control over the ICT sector. For one, the state oil company, Sonangol, owns 3 of the country’s 18 ISPs (MSTelcom, Nexus, and ACS) and is a major shareholder in 2 other companies—UNITEL and Angola Cables, the former of which is the country’s largest ISP. Sonangol’s telecom subsidiary, MSTelcom, discloses its full ownership of Nexus and ACS in: Sonangol Notícias, “9º Aniversário da Mstelcom: Ligando o País e o Mundo,” August 2008, nº 17, Sonangol.

10

The national telecom company, Angola Telecom, an ISP itself, is also a major shareholder in Angola Cables, with 51 percent.

11

Mobile phone services are provided by two private operators, UNITEL and Movicel, both of which have indirect ownership ties to the government. For example, 75 percent of UNITEL, the larger mobile phone operator with 80 percent of the market, is held by three entities: state-owned Sonangol; a business venture run by the president’s lieutenant general, Leopoldino do Nascimento; and the president’s billionaire daughter, Isabel dos Santos, according to investigative reports. Both the general and Ms. dos Santos sit on the board of UNITEL.

12

Meanwhile, 80 percent of Movicel is split between five ostensibly private Angolan companies—Portmill Investimentos e Telecomunicações with 40 percent, Modus Comunicare with 19 percent, Ipang-Indústria de Papel e Derivados with 10 percent, Lambda with 6 percent, and Novatel with 5 percent—that have majority shareholders who are senior officials within the president’s office. For example, the majority shareholders of the Angolan investment company Lambda include Minister of Telecommunications and Information Technologies José Carvalho da Rocha, his deputy, and members of both their families. The remaining 20 percent of Movicel’s capital is held by two state enterprises, Angola Telecom and Empresa Nacional de Correios e Telégrafos de Angola, with 18 percent and 2 percent, respectively.

13

The 2011 Law on Electronic Communications and Information Company Services further enhances the government’s ability to control the country’s ICT sector. On paper, the law aims to ensure that ICTs in Angola are developed to play a fundamental role in ensuring citizens’ universal access to information, transparency in the public sector, and participatory democracy. It also sets broader goals of poverty alleviation, competitiveness, productivity, employment, and consumer rights. Nevertheless, this legislation includes several provisions that, if implemented with bad intentions, can threaten online freedom. In particular, the law’s provision for universal access to information is dependent upon the state’s responsibility “in the creation and promotion of conditions that enable
all citizens to access ICT." Accordingly, the law enables the head of government to "intervene when internet service providers jeopardize their social functions or there are situations that gravely compromise the rights of subscribers or users." Because the law does not define "the social functions" or "situations" that could be compromised or the scope of intervention allowed, analysts believe that the law empowers the president to control the ICT sector at will.

**Regulatory Bodies**

The Ministry of Post and Telecommunications (MCT) is responsible for oversight of the ICT sector, while the Angolan Institute for Communications (INACOM), established in 1999, serves as the sector’s regulatory body. Reporting to the MCT, INACOM determines the sector’s regulations and policies, sets prices for telecommunications services, and issues licenses. On paper, the regulatory body was set up as an independent public institution with both financial and administrative autonomy from the ministry, though in practice, its autonomy is fairly limited. According to reports by the ITU and World Bank, INACOM is not autonomous in its decision making process, in part due to the ministerial appointment of the director general who can be dismissed for any reason. In addition, the MCT has been known to influence staff appointments, while other ministries are often involved in sector policy, leading to politically influenced regulatory decisions.

**Limits on Content**

*No websites were blocked during the coverage period, though government requests to remove content from the internet were reported for the first time. An independent online news outlet received calls from government officials with directives to tone down or refrain from reporting on certain issues. Meanwhile, youth groups have increasingly flocked to Facebook to call for protests against government corruption, reflecting a weakening culture of fear within civil society.*

**Blocking and Filtering**

To date, there have been no known incidents of the government blocking or filtering ICT content in Angola, and there are no restrictions on the type of information that can be exchanged through digital media technologies. Social media and communications apps such as YouTube, Facebook, Twitter, and international blog-hosting services are freely available. Nevertheless, censorship of news and information in the traditional media sphere is common, leading to worries that similar efforts to control the information landscape will eventually spillover to the internet. In a concerning development, the independent online news outlet *Club-K* reported in July 2015 that the Angolan authorities had been seeking technical assistance from North Korea to restrict access to critical websites.  

20 Assembleia Nacional, *Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação* (Lei nº 23/11), art. 5.
Content Removal

During the coverage period, government requests to remove content from the internet were reported for the first time in Angola. In one case, the request was extralegal, originating from a military general who arrested a Facebook user in April 2015 for a critical post about the general (see “Prosecutions and Detentions for Online Activities”). The Facebook user was forced to take down the offending post and to apologize in exchange for his release.25

In May 2015, a court found journalist Rafael Marques de Morais guilty of criminal defamation for his 2011 book implicating the Angolan military with torture and corruption in the country’s diamond industry (see “Prosecutions and Detention for Online Activities”). In addition to a six-month suspended prison sentence, the court ordered all copies and references of de Morais’s book to be removed online.26 Given the impossibility of the task, observers believe the court intended to find a way to send de Morais to prison later down the road.

Otherwise, there were no reported issues of intermediary liability for service or content providers. Predominant state ownership of the majority of Angola’s news outlets likely preempts the need for legal or administrative forms of censorship or content removal. According to an independent analyst, however, the government has been known to deliberately take down its own content when the authorities have wanted to prevent the public from accessing certain government information, such as specific laws.

Media, Diversity, and Content Manipulation

As a result of low rates of ICT access, radio, television, and print outlets—which are subject to high levels of government interference—remain the primary sources of information for the majority of Angolans. The president and members of the ruling People’s Movement for the Liberation of Angola (MPLA) party own and tightly control a majority of the country’s media outlets, including those that are the most widely disseminated and accessed. Of the dozen or so privately owned newspapers, most are held by individuals connected to the government. The state media sector is comprised of the only daily newspaper in the country, Jornal de Angola, the broadcasting company Rádio Nacional de Angola, the Angolan Public Television (TPA), and the news agency Angop. All of these media outlets have websites of their own, none of which allow for comments from readers, enabling them to maintain their role as government mouthpieces.

Independent news outlets critical of the government do exist, with Folha8 being the most prominent, though its audience is reached primarily through its print publication. An online portal based in Portugal launched in 2013, Rede Angola,27 has become one of the main sources of alternative and independent online news on Angola, alongside the Maka Angola and Club-K news blogs. Nonetheless, the online information landscape lacks diversity and is unable to represent a variety of groups and viewpoints throughout the country due to both the concentration of internet access in urban areas and the limited space for critical voices in Angola’s general media sphere.

According to internal sources, some independent online news outlets receive regular calls from

25 Interview by Freedom House consultant in May 2015.
26 Paul Gallagher, “Celebrities join signatories calling on Angolan president to drop prosecution of blood diamonds author Rafael Marques de Morais,” Independent, June 2, 2015, http://ind.pn/1hsfGbM.
27 Rede Angola website: http://www.redeangola.info/.
government officials with directives to tone down or refrain from reporting on certain issues. For example, in 2015, editors at the news blog, *Rede Angola*, reportedly received instructions from the authorities not to publish any news about the ongoing defamation case against journalist and blogger Rafael Marques de Morais.  

Self-censorship is pervasive and commonly practiced by journalists in both state-run and private print outlets, though bloggers and social media users are less reluctant to express criticism of the president and ruling party. In the past few years, the internet and social media have become the last frontier for independent voices, with journalists, activists and opposition parties increasingly turning to digital platforms as a means to sidestep the country’s longstanding restrictions on traditional media. Bloggers and internet users have been generally less fearful of expressing themselves and discussing controversial topics online than they might be offline. Nevertheless, there have been anecdotal reports of online self-censorship becoming more prevalent, reinforced by recent attacks on online journalists (see “Intimidation and Violence”). In addition, taboo topics related to corruption, abuse of power, land grabs, police brutality, and demolitions are often avoided.

The economic viability of independent outlets, both online and in print, is constrained by the lack of advertising revenue from both state and private sources, since it is often denied to news outlets that publish critical stories about the government. According to an Angolan media observer, the independent news blog *Rede Angola* struggled to receive advertising revenue from both private and public sources in 2014 and 2015 due to the critical cartoons it often publishes. It has only managed to stay afloat through financing from its wealthy owner, an Angolan media mogul.

**Digital Activism**

Despite the limited diversity of online news and content in Angola, social media has become the leading platform for citizens to criticize the government and react to alleged wrongdoings. Youth groups in particular have increasingly flocked to Facebook to call for protests against government corruption, reflecting a weakening culture of fear within civil society. Throughout 2014, members of the Facebook group Central Angola 7311 (referring to March 7, 2011, the date of the first organized, nonpartisan protest in 35 years) planned a series of flash mob demonstrations via text message at government ministries to protest restrictions on freedom of expression and assembly. The authorities quickly dispersed each protest within minutes, often with tear gas and other violent means, but not before young protestors could document the protests (as well as the police response) through video and photographs, which they subsequently posted online to garner further attention to their movement. While the protests have yet to result in major political or social outcomes, Central Angola 7311 members contend that their mobilization efforts are building a foundation for further citizen activism.

---

28 Based on interviews with anonymous online journalists and editors.
29 Based on interviews with internet users and bloggers.
30 Central Angola 7311, website, [http://centralangola7311.net/](http://centralangola7311.net/); Central Angola 7311-APagina, Facebook Cause Page, [http://on.fb.me/1VGCp7Y](http://on.fb.me/1VGCp7Y).
Violations of User Rights

The Angolan government increasingly focused its attention on critical comments posted on social media platforms, arresting one user for a Facebook post in April 2015. Leaked Hacking Team emails in July 2015 led to heightened concerns over unlawful surveillance of online and mobile communications. Online activists and critical news outlets were targeted for harassment and technical violence.

Legal Environment

The Angolan constitution provides for freedom of expression and the press, and the country was one of the first in Africa to enact a freedom of information law in 2002, though in practice, the government and authorities routinely flout these rights. In addition, stringent laws regarding state security and defamation run counter to constitutional guarantees, such as Article 26 of the 2010 state security law that penalizes individuals who insult the country or president in “public meetings or by disseminating words, images, writings, or sound” with prison sentences of up to three years. The 2006 press law holds authors, editors, or directors of a publication criminally liable for libelous content. If the author does not reside in the country or the text is not signed, the law establishes the circumstances in which the editor, director, or both may be held criminally responsible for grievous content. Defamation is also a crime punishable by imprisonment, while politicians enjoy immunity from all prosecution. Meanwhile, the judiciary is subject to considerable political influence, with Supreme Court justices appointed to life terms by the president and without legislative approval.

A Law on Electronic Communications and Services of the Information Society was enacted in August 2011 that provides for citizens’ rights to privacy and security online, among other provisions regulating telecommunications. Nevertheless, the law also includes problematic aspects that may infringe on internet access, such as enabling the president as the head of government to “intervene when internet service providers jeopardize their social functions or there are situations that gravely compromise the rights of subscribers or users” (see “ICT Market”). Because the law does not define “the social functions” or “situations” that could be compromised or the scope of intervention allowed, analysts believe that the law empowers the president to control the ICT sector at will.

Prosecutions and Detentions for Online Activities

In the past year, the Angolan government increasingly focused its attention on critical comments posted on social media platforms, arresting one user for a Facebook post in April 2015. The Facebook post in question was the user’s account of his abuse at the hands of a military general, prompting the general to arrest the Facebook user for the post. Detained in a military prison without charges, he was released a week later only after he agreed to take down the offending post.

In May 2015, the ongoing defamation charges against investigative journalist and blogger Rafael Marques de Morais culminated in a guilty verdict, which carried a six-month suspended prison sen-

---

35 Art. 71, 2, Assembleia Nacional, Lei de Imprensa (Lei 7/06), 2006.
36 Art. 71, 2, Assembleia Nacional, Lei de Imprensa (Lei 7/06), 2006, art. 26º, 2.
tence and orders to remove all copies and references of his investigatory exposé from the country and on the internet. De Morais had been initially charged in 2013 with nine counts of defamation against military generals for his 2011 book that accused the Angolan military of crimes against humanity in its dealings with the country’s blood diamond industry, though his prominence as a blogger likely inflamed efforts to silence him.\(^\text{38}\) While the trial could have resulted in a prison sentence of up to nine years and over US$1 million in fines, the court’s absurd order to remove all references of de Morais’s book from the internet was viewed by observers as an effort to imprison the journalist later down the road, since it would be virtually impossible for de Morais to ensure compliance.

Surveillance, Privacy, and Anonymity

The government's ability to monitor and intercept the data and communications of Angolan citizens without adequate oversight is a major concern, particularly among human rights activists and journalists, though the full extent of the government’s surveillance capabilities and practices is unknown. Sophisticated spyware discovered on an investigative journalist’s laptop in 2013 that logged his activities suggests that, at a minimum, the government engages in the targeted surveillance of select individuals (see “Technical Attacks”).\(^\text{39}\)

In June 2015, Wikileaks published leaked emails the Italian surveillance company Hacking Team, which revealed efforts by Angola’s intelligence agency, SINSE, to acquire Hacking Team’s notorious Remote Control System (RCS) sometime in 2013.\(^\text{40}\) Sold to numerous repressive regimes around the world, the RCS spyware has the ability to steal files and passwords and intercept Skype calls and chats, among other malicious features. No further evidence surfaced as to whether the Angolan government eventually purchased or installed the spyware.

An April 2013 investigative report by the independent online news outlet Club-K revealed plans by intelligence and state security services to implement an electronic monitoring system that could track email and other digital communications. According to Club-K, the sophisticated monitoring equipment had been imported from Germany, and the deal included the services of German technicians who would assist in the system’s installation on a military base in Cabo Ledo, home of the Technical and Operational Battalion (Batalhão Técnico Operacional–BATOPE).\(^\text{41}\) In early 2014, an anonymous researcher acquired corroborating information from military sources that the monitoring system had been installed at the BATOPE base around September 2013.\(^\text{42}\) Further evidence surfaced in November 2013 of at least one major ISP hosting a spyware system directly on its server, as part of the German company setup. No new information regarding the surveillance system and its use has since come to light.\(^\text{43}\)

Meanwhile, SIM card registration requirements announced in early 2015 threaten to constrain the ability of mobile phone users to communicate anonymously. The strong presence of the state in the


\(^{42}\) Anonymous Freedom House researcher, March 2014.

\(^{43}\) According to FH interviews.
Angola

Ownership structure of Angola’s telecoms, particularly of mobile phone operators, suggests that the authorities are likely able to wield their influence over service providers and require ICT providers to assist in the monitoring of communications, if desired. For instance, the top adviser to the head of the Intelligence Bureau at the Presidency, General Leopoldino do Nascimento, is also the chairman and shareholder of Unitel. Meanwhile, the head of the Intelligence Bureau, General Manuel Hélder Vieira Dias “Kopelipa,” holds a majority share (about 59 percent) in Movicel. The deputy CEO and Chief Technology Officer of Unitel, Amílcar Safeca, is the brother of Aristides Safeca, the secretary of ICTs who in turn is a shareholder of Movicel. Such interweaving of political and business interests through family connections is compounded by the lack of rule of law.

Intimidation and Violence

Violence against journalists in the traditional media sphere is unfortunately common in Angola, and online activists have been increasingly targeted. In 2014, youth movement protestors of the Central Angola 7311 Facebook group routinely reported abuse and torture while in detention for their participation in antigovernment protests. Online writers and investigative journalists, including Rafael Marques de Morais, are also frequently subject to intimidation and attacks for their work, though no incidents were reported during the coverage period.

Technical Attacks

Independent and diaspora news websites are frequently targeted by technical attacks, such as hacking and denial-of-service (DoS) attacks, particularly during periods of political contestation. In 2015, the critical news blog Maka Angola was attacked and taken down for several days at a time in the lead-up to the criminal defamation case against the outlet’s owner and investigative journalist, Rafael Marques de Morais, who has been a frequent target of technical violence. In 2013, de Morais’s personal laptop was attacked with customized malware, which international experts linked to a multinational with strong ties to Angolan military officials.

---

44 General Kopelipa openly represents Portmill, Investimentos e Telecomunicações, which holds 40 percent of Movicel. He is also a co-owner of Banco Espírito Santo Angola which is a major Movicel investor as well. In 2010, journalist Rafael Marques de Morais found in an investigation that Portmill had been set up by Gen. Kopelipa, Gen. Leopoldino do Nascimento and the current vice-president of Angola, Manuel Vicente.


47 Gunter, “Digital Surveillance in Angola and Other ‘Less Important’ African Countries.”
Argentina

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td>Free</td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>27</td>
<td>27</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- In December 2014, Congress passed the Argentina Digital Law, which aims to guarantee socially and geographically equitable telecommunications services to all citizens. Although the law contains several positive provisions, such as the establishment of net neutrality protections, it sparked criticism from academics and civil society organizations during the debate process for vague wording and wide powers conferred to the regulatory authority. The Communications Secretariat is currently developing regulation to implement the law (see Availability and Ease of Access).

- In October 2014, the Supreme Court issued an important ruling on intermediary liability, stating that search engines should not be held liable for linking to user-generated content that violates rights or infringes copyright, as long as the search engine complies when a judicial order demands that it take down said content (see Content Removal).

- After using Twitter to alert the public about the death of the prosecutor investigating a 1994 terrorist bombing in Buenos Aires, journalist Damian Pachter fled the country out of fear for his safety. In what was widely seen as a violation of the journalist’s privacy, the national news agency published his flight itinerary, which included personal information, and the official Twitter account of the Argentine presidential palace reposted it (see Intimidation and Violence).
Introduction

Although plagued by slow internet speeds and high prices, Argentina has one of the highest internet penetration rates in Latin America. During the coverage period the government did not block or filter the internet, and several positive court rulings on intermediary liability established a judicial notice and takedown system. Despite these positive developments, several bills under consideration in the legislature have the potential to restrict internet freedom by leading to the removal or blocking of content. Online journalists in Argentina reported instances of harassment over the past year, including a couple of notable cases, however levels of harassment and violence towards journalists are lower than in many other countries in the region.

In December 2014, Congress passed a law known as the “Argentina Digital Law,” the goal of which is to guarantee socially and geographically equitable telecommunications services to all citizens. Some of its articles include the declaration of ICT development and regulation as a public service, the establishment of net neutrality, and the creation three new regulatory authorities. The law was passed despite criticism for its vague wording, wide powers conferred to the regulatory authorities, and insufficient protection of personal data, among other issues. The Communications Secretariat is currently developing the regulation for the law, which will define key aspects, such as how the regulatory authorities will be organized.

During 2013 and 2014, four different bills that could regulate blocking, filtering, or removal of content in some way were introduced in the Argentine Congress. As of May 2015, three of these bills were stalled in the early stages of the legislative process and had not yet been brought up for a vote. Among these bills was a bill known as “The Right to be Forgotten,” which would allow users to request that internet intermediaries eliminate or block publications that could violate their right to privacy, honor, and image, so long as the content was not deemed to be of public interest. Another bill that would require ISPs to block content that in any way encourages human trafficking was approved by the Representative’s Chamber and was under debate in the Senate as of May 2015.

Although there is not a specific legislative framework that regulates intermediary liability, the Supreme Court issued an important ruling, followed by two other similar decisions, emphasizing the importance of freedom of expression online. It stated that search engines should not be held liable for linking to third-party content that violates rights or infringes copyright, as long as they comply when a judicial order demands that they take said content down.

In 2015, the investigation into the 1994 terrorist attack on the Jewish Mutual Aid Society in Buenos Aires became a focal point on social media, especially after a prosecutor investigating the bombing was found dead the night before he was due to testify before Congress. People took to social

---

4 “Nisman se presentará en el Congreso para explicar su denuncia por la causa AMIA,” [Nisman will make a presentation in the Congress to explain his accusation on the AMIA cause] Télam, January 18, 2015, [http://bit.ly/1bADDeh](http://bit.ly/1bADDeh); “El fiscal Alberto
Argentina

media to organize a demonstration demanding justice, which gathered hundreds of thousands of people.5

Damian Pachter, the journalist whose tweet first broke the story of the prosecutor’s death, claimed that he was under government surveillance and fled the country out of fear for his own safety.6 The national news agency published his flight itinerary, which included personal information7 and which was re-tweeted by the official Twitter account of the Argentine presidential palace.8 The government argued that they published the flight information in order to show that Pachter had a return flight to Argentina and thus argue that he was not fleeing for his life. Many critics thought that the government’s decision to disseminate Pachter’s personal flight information constituted a significant violation of the journalist’s privacy.9

Obstacles to Access

Access to the internet has increased consistently in Argentina during the last decade. However, there are still infrastructural weaknesses that contribute to a digital gap, especially between urban and rural areas, with the majority of internet connections concentrated in urban areas. Several governmental initiatives aim to improve this situation. Congress recently passed the Argentina Digital Law, which classified ICT development and regulation as a public service, established net neutrality protections, and created new regulatory bodies to oversee ICTs. Some civil society groups have criticized the law for vague wording and insufficient data protection, among other issues.

Availability and Ease of Access

Over the past decade, internet access has consistently been on the rise in Argentina. Statistics published by the International Telecommunications Union (ITU) showed a 65 percent internet penetration rate in the country by the end of 2014, up from 60 percent in 2012 and 34 percent in 2009.10 In December 2014, Congress passed a law known as the Argentina Digital Law,11 which aims to guarantee socially and geographically equitable telecommunications services to all citizens. The law

8 Casa Rosada Twitter, Twitter post, January 24, 2015, 4:32 PM, http://bit.ly/1BoTrCI.
classifies ICT development and regulation as a public service, establishes net neutrality protections, and aims to enable access to ICTs throughout the country through a variety of measures, such as promoting investment in a Universal Service Fund that goes toward improving infrastructure and fostering interconnection among providers. The Communications Secretariat is currently working on the regulation of the law.

The National Institute of Statistics and Census in Argentina (INDEC) reported that, as of September 2014, there were 13.3 million residential internet subscriptions—an increase of 11 percent from 2013. The vast majority of these subscriptions were broadband, with dial-up connections accounting for only 30,405 subscriptions, less than one percent of the total. The INDEC also reported that in September 2014 there were 2.3 million internet subscriptions belonging to organizations, which represents a 15 percent increase over the previous year. Almost 400 of these organizations, which include schools, libraries, and nongovernmental organizations, benefited from free internet access.

An interactive map created by the government of Buenos Aires shows the location of about 300 public access Wi-Fi spots in the city of Buenos Aires.

Measurements of internet speed in Argentina vary, but a range of sources show that the country lags well behind global averages in broadband speed. The average broadband speed in Argentina was 4.4 Mbps during 2014, although the Cisco Visual Networking Index has said that this speed is expected to reach 15 Mbps by 2019. In comparison, the average global speed was 20.3 Mbps by the end of 2014 and is projected to reach 42.5 Mbps by 2019. In February 2014, Netflix ranked the country among the slowest at both the regional and global levels, with speeds of 1.2 to 1.9 Mbps depending on the internet service provider (ISP). Speeds also vary significantly by region: Ookla's Net Index estimated a speed of 10 Mbps in Buenos Aires with significantly lower speeds in other provinces, such as 6.7 Mbps in Santa Fe, 4.6 Mbps in Tucumán, and 3.0 Mbps in Mendoza.

Mobile phone penetration continues to be high in Argentina. The ITU reported around 66 million mobile phones actively in use, representing a penetration rate of 159 percent. Overall, the trend over the five years has been increased penetration, with the ITU showing a 26 percent increase in the number of mobile subscriptions between 2009 and 2014.

Despite the increase of internet connections in Argentina, infrastructural weaknesses and high prices...
Argentina

put internet access beyond the reach of certain segments of the population, particularly in rural areas. Connection subscriptions are concentrated in urban areas, with the majority found in Buenos Aires, Córdoba, Santa Fe, and Mendoza.22 Whereas in December 2014 the City of Buenos Aires claimed a rate of 1.4 broadband connections per inhabitant according to INDEC data, Formosa province claimed a meager 0.1 connections per inhabitant.23

High prices constitute a major obstacle to internet access in Argentina. According to a 2014 ITU report,24 the average broadband plan costs US$40 per month,25 whereas the average salary in the country is around US$1,200.26 In 2013, the Technology and Society Centre of San Andrés University published a report placing Argentina’s cheapest internet access plan among the most expensive ones in the region.27 When asked why they lacked access to internet, 56 percent of respondents cited affordability as one of the reasons.28 Whether or not the Argentina Digital Law will decrease prices or increase access remains to be seen. Although the state does not set the price of internet subscription fees, the new law requires that ICT providers set their prices in a “fair and reasonable” way.29

Mobile subscription prices are also very high in Argentina compared to neighboring countries. The World Economic Forum labeled Argentina as one of the most expensive countries in Latin America for mobile services in 2014.30 Since August 2014, the government has offered an alternative prepaid plan, less expensive than those offered by companies, which includes text messages, multimedia messages, mobile internet, and free calls to one number.31 After an increase in data consumption because of 4G, mobile phone companies sparked complaints by increasing their plan fees.32 Ultimately, the National Communications Commission imposed a fine on one of these operators for the illegitimate change in its fees without notifying users, and ordered the operator to go back to the original fees.33

During the coverage period, the Argentina Connected Plan, a five-year government initiative started in 2010 in order to improve connectivity and access, entered its final year. One of the initiative’s most

---

23 Guillermo Tomoyose, “Un mapa interactivo muestra el nivel de acceso a Internet en la Argentina.”
26 Converted at the official rate. This is INDEC’s estimate, pondering an average $12,365 for public sector employees, and $6461 for informal work. See Daniel Sticco, “Para el INDEC, la suba de salarios duplicó a la tasa de inflación,” [According to INDEC, the rise in salaries doubled the inflation rate] Infobae, March 4, 2015, http://bit.ly/1K9HWht.
27 Hernán Galperín, “Broadband Prices in Latin America and the Caribbean” (working paper, Universidad de San Andrés, Buenos Aires, Argentina, 2013) 6, Figure 1.
29 Argentina Digital Law, art. 48.
Argentina

important components is the Federal Network of Optical Fiber (Red Federal de Fibra Óptica), a project contracted to the state-owned company AR-SAT to extend approximately 58,000 km of fiber-optic cable across the country as a means of facilitating internet access for 97 percent of the population. Although there have been concerns over the pace of the project’s development throughout the years, in May 2014, the government announced that the Ministry of Planning had overseen the construction of 30,000 km of fiber-optic network.

The Ministry of Federal Planning, Public Investments and Services reported in September 2014 that it oversaw the establishment of 173 Access to Knowledge Centers, public spaces that provide free access to ICTs, under the Argentina Connected Plan. Also, as a part of this initiative, the first Argentine telecommunications satellite, Arsat-1, was successfully launched in October 2014, and another one, Arsat-2—currently in a testing phase—is expected to launch in 2015.

Another positive policy implemented by the government is the Connect Equality initiative, which began in 2010 and aims to foster digital inclusion by providing a netbook to every student and teacher in public high schools. As of April 2015, more than 4.7 million netbooks had been delivered to students. However, critics have raised questions about the effective use of these technologies for educational purposes, and reports about widespread technical problems remain unresolved.

Restrictions on Connectivity

The Argentine government does not place limits on bandwidth, nor does it impose control over telecommunications infrastructure. There have been no reported instances of the government cutting off internet connectivity during protests or social unrest. There are currently fifteen functioning Network Access Points (NAPs), which help with internet traffic.
ICT Market

There are approximately 760 companies that are licensed to offer internet services in Argentina, which indicates a diverse digital technology spectrum free of onerous obstacles to entry. For a company to offer internet services, it must first obtain a license from the National Communications Commission (CNC). The application fee is fairly reasonable at ARS 5,000 (US$543).

Although generally speaking there are no onerous obstacles to entering the ISP market, a study by telecommunications expert Martín Becerra shows that by 2013 more than 85 percent of the broadband market was concentrated in three companies, Telefónica, Telecom, and Grupo Clarín. It is still unclear what effect the Argentina Digital law will have on the ISP market and whether it will enable further concentration. Under the Argentina Digital Law, the licensing system for ICT providers may change, but regulation governing these potential changes has yet to be announced.

The mobile market is also concentrated in the hands of a few companies, namely Movistar, Claro, and Personal. In October 2014, the government started spectrum auctions for 4G mobile phone frequency, and revealed that it had received bids of over US$2.2 billion based on the participation of four companies: Movistar (Telefónica Móviles Argentina), Personal, Arlink (property of group Vila-Manzano), and Claro (AMX Argentina). This auction process placed Argentina among the four countries of the region with the most spectrum assigned, according to the association 4G Americas. However, despite the initiation of 4G networks, the Cisco Visual Networking Index 2014-2019 estimates that only 10 percent of users in Argentina will be using 4G networks by 2019.

Regulatory Bodies

The Argentina Digital Law, passed in December 2014, significantly changed the country’s ICT regulatory structure by subsuming the Communications Secretariat and Argentina’s historic regulator, the National Communications Commission (CNC), into three new regulatory bodies. Although regu-
latory bodies have been subject to some government intervention in past years,\textsuperscript{52} the CNC, prior to being dissolved, had a reputation for being a relatively independent, public, decentralized body.

The Argentina Digital Law created three new regulatory authorities – the Federal ICT Authority, the Federal Council of Telecommunications and Digitalization Technologies, and a Bicameral Commission for Promotion and Monitoring of Audiovisual Communication and Telecommunication and Digital Technologies. Under the new law, the Federal ICT Authority and the Federal Council of Telecommunications and Digitalization Technologies will absorb the structure and functions of the CNC.\textsuperscript{53}

The procedure for the transfer of the CNC to the newly created application authorities will be determined by the law’s regulation, which was still being developed as of June 2015.

Some critics of the Argentina Digital Law worry that the three regulatory authorities will have overly broad powers; for example, the power to grant licenses or take them away, decide which public policy will be implemented to ensure universal service, and impose specific obligations on providers with “significant market power.”\textsuperscript{54} Also, the law leaves many aspects to be determined by the regulation, which these authorities will later enforce.\textsuperscript{55}

In April 2014, the Communications Secretariat created the Commission for Internet Policy (CAPI), with the aim to foster “participation of different actors to design a national strategy for internet governance ...[and] to contribute to a better representation of Argentina in international organizations and forums.”\textsuperscript{56} However, this is not a regulatory body, and it has yet to be determined whether its resolutions will be binding.

Any website ending in “.ar,” must be registered with NIC.ar, the executive body that regulates and registers domain names. As of June 2015, registration of any domain ending in “.com.ar” required an annual fee between ARS 65 and ARS 450 (US$7 and US$49) per year.\textsuperscript{57} The rationale behind this change was to prevent people from registering for domain names they are not going to use. Although the fees are reasonable considering that the average monthly wage is ARS 10,800 (US$1,173),\textsuperscript{58} domains were previously free, and the new policy could deter some users.\textsuperscript{59}

\textsuperscript{52} D.P, “Pressed,” The Economist, 8/25/2010, \url{http://econ.st/1lwG1ve}.
\textsuperscript{53} Ley No. 27078, art. 79 and 87.
\textsuperscript{54} Ley No. 27078, art. 12, 20 and 46.
\textsuperscript{57} NIC Argentina, Registration Fees, \url{http://bit.ly/1fac2e}.
\textsuperscript{58} This is INDEC’s estimate, pondering an average $12,365 for public sector employees, and $6461 for informal work. See Daniel Sticco, “Para el INDEC, la suba de salarios duplicó a la tasa de inflación,” [According to INDEC, the rise in salaries doubled the inflation rate] \emph{Infobae}, March 4, 2015, \url{http://bit.ly/1K9HwTc}, Conversions to USD were conducted using the OANDA rate as of August 5, 2015 \url{http://www.oanda.com/currency/ converter/}.
\textsuperscript{59} Marcelo Bellucci, “Habrá Que Pagar Por Registrar un Dominio en Internet en Argentina” [There Will Be a Charge to Register a Domain Name in Argentina] \emph{Clarín}, February 25, 2014, \url{http://clarin/1qzB8Wk}, “El Registro de Dominios en Internet Dejará de Ser Gratuito Desde Marzo” [Registering Domains on the Internet Will Not Be Free As of March], \emph{Télam}, February 24, 2014, \url{http://bit.ly/1encQkq}. 

45 www.freedomhouse.org
Argentina

Limits on Content

During late-2014 and early-2015, three Supreme Court rulings on intermediate liability set a valuable precedent for freedom of expression. On the other hand, several bills that proposed blocking or removal of certain content were introduced in Congress in 2014. The introduction of such extensive legislation to expand blocking, filtering, and takedown of content raised concerns among free speech advocates, who worried that the broad wording of these initiatives could limit internet freedom and lead to restrictions on politically and socially relevant content. Although most of these bills have stalled in the early stages of the legislative process, they could still be debated before the end of the 2015 legislative session on November 30th. One bill, which would block content deemed to promote human trafficking, has been approved by the Chamber of Deputies and is under debate in the Senate.

Blocking and Filtering

Argentine internet users have access to a wide array of online content, including international and local news outlets, as well as the websites of political parties and civil society initiatives. YouTube, Facebook, Twitter, and international blog-hosting services are freely available. There is no automatic filtering of internet sites, web pages, platforms, social media sites, or blogs. Law 25.690, however, requires ISPs to provide software that can allow users to choose to limit their own access to “specific websites.” Other laws at the municipal or state level mandate the blocking of pornographic websites in public locations, such as libraries and educational institutions.

During the coverage period, several controversial bills that regulated filtering, blocking, and content removal in some way were debated in Congress (see Content Removal for more information on bills related to the removal of personal data or discriminatory content). As of June 2015, only one of the bills—a bill that proposes the blocking or removal of content that promotes human trafficking—was under consideration in the Senate, after having been approved by the Chamber of Deputies. This bill (6943-D-2013) would ban all content that promotes human trafficking and would forbid all publications that promote commercial sex work. If passed, a regulatory body within the executive branch would have the power to monitor media to spot prohibited publications and request the blocking or removal of the content in question with no mechanism for judicial oversight.

Some civil society groups opposed this bill on the grounds that the language is overly broad. The bill’s stated aim is to stop human trafficking, but the language of the bill prohibits any communication related to the commercial offer of sexual activity, which is not illegal in Argentina. Other critics worry that the bill does not include a mechanism for judicial review and argue that allowing the regulatory bodies to order the blocking and removal of content without a court order creates a dangerous precedent.

---

60 Ley No. 25.690, http://bit.ly/1I0q2JX.
65 ADC, “Comentarios sobre el proyecto de eliminación de mensajes que fomenten la explotación sexual,” [Comments on the
Argentina

In the past few years, there have been cases of blocking and filtering of allegedly defamatory material and copyright protected content, including cases of blocking or content removal on grounds of copyright infringement on content sharing platforms.66 In a June 2014 civil case initiated by the Argentine Chamber of Phonogram Producers (CAPIF), a civil court ordered ISPs to block access to IP addresses associated with The Pirate Bay, a website that facilitates peer-to-peer (P2P) filesharing using BitTorrent protocol, on the grounds that The Pirate Bay included links to copyright protected content.67 The blocking of the platform was unsuccessful, however, as it was possible to access it from other websites, including from the CAPIF website, which was hacked to redirect users to The Pirate Bay platform.68 One of the most controversial aspects of the decision was that the blocking of the platform in Argentina also affected Paraguay, since that country’s connection to the internet goes through Argentina and Brazil.69

Argentina boasts a wide availability of social media and international blog-hosting services, like YouTube, Facebook, Twitter, and others. There are no known cases of blocking social media for political reasons. Although a few policymakers proposed limiting social media sites in 2013 in the wake of protests and a wave of looting, this initiative was widely criticized and quickly defeated.70

Content Removal

Between October 2014 and December 2014, three court rulings on intermediary liability expanded freedom of expression by ensuring that intermediaries did not have to preemptively screen or censor content. These rulings inspired a bill to create a framework for intermediary liability, which was introduced in May 2015 to the Argentine Congress. During the 2014 legislative session, three bills that would have regulated blocking and content removal were introduced but had not yet been debated or voted on in the legislature as of May 2015.

The most important judicial decision regarding intermediary liability occurred in October 2014, when the Supreme Court confirmed the appellate court’s decision to overturn a lower court’s ruling, which required search engines to eliminate certain sexual and erotic content related to the petitioner, the celebrity Belén Rodriguez.71 The lower court, whose opinion was challenged in an appellate court bill to ban messages that promote sexual exploitation] November 12 2014, http://bit.ly/1yA97T4.


71 Supreme Court of Justice, “Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios.”
fore reaching the Supreme Court, argued that the unauthorized use of sexually-explicit photographs of Rodriguez violated her honor and her right to those images and demanded that the search engines block the sites containing these photographs and offer compensation. The Supreme Court rejected this argument, stating that search engines should not be held liable for linking to third-party content that violates rights or infringes copyright, as long as they are not negligent—meaning that they comply if a judicial order demands that they take said content down and they take down or block “manifestly unlawful” content, such as child pornography or genocide incitement. The Court emphasized online freedom of expression in its ruling, and argued that using a strict liability regime would harm this freedom by incentivizing intermediaries to monitor and preemptively take down any potentially illegal content. The Court cited international human rights agreements, including the American Convention of Human Rights, which prohibits prior censorship except in “absolutely exceptional cases.”

A few months later, the Supreme Court reinforced this precedent by deciding that intermediaries were not liable in two similar cases in which celebrities were suing search engines for providing links to sexually explicit content. The standard that the court set in these decisions of only requiring preemptive blocking in cases of “manifest unlawfulness” is somewhat imprecise, and lower courts in Argentina’s legal system are not obligated to follow Supreme Court precedent; however, this ruling is still a valuable precedent for freedom of expression.

As of May 2015, Argentina still lacked any specific legal framework to regulate intermediary liability. In this context, the Supreme Court’s rulings on intermediary liability in 2014 were especially important, as they provided a precedent that may encourage the lower courts to rule more consistently against strict intermediary liability. In the past, judicial rulings on intermediary liability have been inconsistent and have generated an environment of uncertainty. Many past judicial rulings deferred to the general torts framework when deciding a case, which sometimes posed risks to rights online and resulted in very diverse and variable case law. Some judicial rulings in the past have held intermediaries liable on the grounds that the intermediaries’ activity is an inherently “risky” activity or on the grounds that the intermediaries were violating Argentina’s 90-year-old intellectual property law, which holds anyone who reproduces copyrighted content liable.

Inspired by the Supreme Court rulings on intermediary liability, Senator Liliana Fellner introduced a bill in May 2015 to Congress that would establish the general principle that search engines must not be held liable for third party content, and do not have to preemptively monitor or control content. The law establishes a judicial notification procedure and says that intermediaries will only be held liable if, after being notified about unlawful content, they fail to take appropriate measures. Never-
Nevertheless, similar to the judicial rulings, the legislation would make an exception for “manifestly unlawful” content, which intermediaries would be required to remove upon notification by an individual user even without judicial participation. Un fortunately, the legislation establishes a rather vague and broad definition of manifestly unlawful content, citing as examples content that facilitates or instigates the commission of crimes; endangers a person’s life or integrity; incites genocide, racism or discrimination; thwarts current judicial investigations; produces severe damage to a person’s honor, privacy or image; or exhibits child pornography. The bill will be under discussion in 2015 in the Senate’s Commission on Systems, Media and Freedom of Expression.

In 2014, two bills introduced in the legislature would require intermediaries to block or remove personal information based on a user’s request. Although neither bill had been debated by mid-2015, they could still be picked up before the legislative year ends on November 30, 2015. Bill 7989, introduced in October 2014, would have established a so-called “right to be forgotten,” allowing users to request that internet intermediaries, including search engines and websites, remove or block publications that could violate their right to privacy, honor, and image, although the bill provided an exception for content of public interest. If the intermediary failed to comply, the bill establishes judicial review to determine whether the content really violated a person’s privacy and, if so, whether the intermediary should be fined.

A second, similar bill introduced in the same month, proposed the elimination of personal information online. If passed, the bill would have enabled users to request that search engines block and remove all personal data that did not affect public interest; however, unlike Bill 7989, this initiative did not propose a judicial review process.

In September, 2014, representatives introduced a bill that would have authorized the National Institute against Discrimination, Xenophobia, and Racism to order site administrators to take down any racist or xenophobic content or messages that undermined or insulted people based on their ethnicity, religion, gender, or sexual orientation. The bill proposed a judicial review process through which courts could impose serious sanctions—even interruption of service—for sites that fail to comply with the content removal request. By mid-2015, the bill hadn’t been debated in the Commission.

However, in July, after the end of the coverage period for this report, a new bill against discrimination integrated this bill along with others and was approved by the Representatives Chamber’s Human Rights Commission. This new bill sparked criticism from civil society and academia because, if
Argentina

passed, it would allow individuals to request that intermediaries block any content that fell under a very broad definition of discriminatory material.90

Media, Diversity, and Content Manipulation

Argentina has a relatively open and diverse online media environment, as well as high rates of social media use. Self-censorship among bloggers and online users is not widespread in Argentina, although some isolated instances of harassment may elicit self-censorship in particular cases (see Intimidation and Violence).

The discriminatory allocation of official advertising, both at the federal and local levels,91 plays a major role in shaping media content in Argentina, and the government has come under fire repeatedly for providing substantial funding through advertising to media outlets that write favorable editorials, while cutting off advertising for critical organizations.92 Nevertheless, it is likely that discriminatory allocation of advertising affects traditional media more than it affects digital media, although the latter, especially in the form of online editions of traditional newspapers, may be affected as well.

There have been multiple rulings by different judicial courts ordering the government to distribute official advertising in an equitable way. In February 2014, Argentina’s Supreme Court ruled that the government must comply with equitable allocation of advertising, and in 2013 the Supreme Court recommended transparent public policy in terms of official advertising.93 However, according to the latest figures published by the executive branch, ten groups, mostly large traditional media organizations, all of whom are allegedly close to the government,94 obtained 50 percent of the total of funds allocated to official advertising.95 Unfortunately, there is little data specific to advertising revenue for digital media or the effect of discriminatory allocation of advertising on the online editions and digital ventures associated with traditional newspapers.

Digital Activism

Argentines continue to use social media as a tool for political mobilization. On November 13, 2014,

Argentina

Social media was crucial in spreading the word about an antigovernment demonstration under the hashtag #13N. Like previous demonstrations, the protest generated considerable social media attention, with people both supporting and mocking the protest online.96

Another relevant demonstration took place after Alberto Nisman, the prosecutor investigating the terrorist bombing of the Jewish Mutual Aid Society in Buenos Aires in 1994, was found dead in his apartment the night before he was scheduled to appear before Congress in order to present information implicating the government in a cover up related to the bombing.97 Organizing under the declaration ‘I am Nisman,’ about 20,000 people gathered to demand justice in a spontaneous demonstration, which generated significant media attention.98 Afterward, several prosecutors convoked another demonstration, demanding justice for Nisman, on February 18, 2015 and drew over 400,000 people through the social media hashtag #18F.99 Government officials criticized the demonstration, which they perceived as an opposition mobilization,100 and on March 1, 2015, government supporters organized a separate demonstration in support of President Cristina Fernández with the hashtag #1M.101

In June 2015, digital activism played a central role in the demonstration #NiUnaMenos.102 After several women were murdered, a group of journalists and activists called for a demonstration to advocate for concrete actions to fight violence against women. The march went viral on social media, with the hashtag #NiUnaMenos (Not One Less),103 and on June 3, 2015, thousands of people gathered in front of the Congress.104 The mobilization had major reverberations on Twitter: during the demonstration the hashtag generated more than 270,000 tweets.105

100 “Cristina Kirchner, sobre la marcha por Nisman: “A ellos les dejamos el silencio, siempre les gustó el silencio”,” [Cristina Kirchner, on the Nisman demonstration: “To them, we leave them silence, they always liked silence”] La Nación, February 11, 2015, http://bit.ly/18wmmE; “Cristina calificó la marcha del 18F como “opositora” y dijo que marcó “el bautismo del Partido Judicial”, [Cristina qualified the 18F demonstration as ‘opposition’, and said it marked the “baptism of the Judiciary”] Ambito, February 21, 2015, http://bit.ly/1yXINQt
102 This mobilization occurred after the end of the coverage period for this year.
103 Facebook, Ni Una Menos, http://on.fb.me/1d7YqE
105 Guillermo Tomoyose, “Del mundo on line a la marcha: el mapa con las repercusiones de #NiUnaMenos en Twitter,” [From
Argentina

Violations of User Rights

Argentina does not suffer from the same high levels of violence against journalists that are seen in many countries in the region. Nevertheless, two incidents of harassment against journalists during the coverage period—a police search of a media outlet’s offices and the release of a newspaper journalist’s personal flight information—raise concerns about intrusions on journalists’ privacy. Overall Argentina has relatively strong privacy protections, and authorities must obtain a judicial warrant before conducting surveillance. In the realm of digital privacy, the National Directorate for Protection of Personal Data, a governmental body under the Ministry of Justice and Human Rights, issued guidelines for best practices in the development of applications that respect users’ privacy rights. These guidelines may help systematize and advance digital privacy rights in the country.

Legal Environment

The Argentine Constitution, which incorporated several international human rights treaties in 1994, guarantees freedom of expression.106 Since 1997, Argentine law has explicitly established online freedom of expression protections;107 these protections were further strengthened and extended to include “the search, reception and dissemination of ideas and information of all kinds via internet services” in 2005 with Law 26032.108

In 2009, the Argentine legislature decriminalized defamatory statements referring to matters of public interest.109 Statements that judges deem not to relate to the “public interest,” however, can still be charged as criminal offenses under the Argentine penal code, with the penalty set as a fine between US$330-$3,320.110 Individuals can also sue for large sums in court on the grounds of defamation. Despite the vague parameters of the law decriminalizing defamation, the Argentine judiciary has frequently ruled against liability for defamation in relevant cases. In August 2013, for example, the Supreme Court ruled that the blogger Jorge Warley could not be held liable for defamation after he was sued by Ariel Sujarchuck, a public official at the University of Buenos Aires, for reposting an article, written by another author, which criticized Sujarchuck.111

Several laws impose criminal and civil liability for online activities, such as intellectual property infringement, fraud, hacking, and child pornography. For example, a law on intellectual property (Law 11.723) holds liable anyone who, by any means, reproduces content that violates this law and establishes sanctions ranging from fines to six years in prison.112 A few laws regarding online activity have generated concern among activists, who believe that the laws, although well intentioned, are too broadly worded and could affect legitimate speech. In November 2013, for example, a law on child

---

110 The law establishes the fine at 3,000-30,000 Argentine pesos. June 2015 conversion rates were used to calculate the equivalent in USD.
112 Law 11.723, art. 71 to 78.
Argentina

grooming, which amended the penal code and established penalties of up to four years imprisonment for online contact with a minor carried out "with the purpose of committing a crime against [the minor's] sexual integrity,"\textsuperscript{113} generated debate among academics and legislators for vague wording.\textsuperscript{114}

In 2008, the Argentine government passed a law on cybercrime (Law 26388), which amended the Argentine Criminal Code to prohibit distribution and possession of child pornography, interception of communications and informatics systems, hacking, and electronic fraud.\textsuperscript{115} Some of the terms used in the legislation have been criticized as too ambiguous, which could lead to overly broad application of the law. Although there are no cybercrime investigative units at the national level, a specialized prosecutor's office was activated in Buenos Aires in 2012.\textsuperscript{116}

Prosecutions and Detentions for Online Activities

Although there were no known cases of detention or criminal prosecution of individuals in 2014 or 2015 expressly related to the dissemination or access of information on the internet, a case against the director of \textit{La Brújula}, a radio station and news website in Buenos Aires province, raised concerns among human rights activists.

In October 2014, the judiciary ordered the search of \textit{La Brújula} to uncover the sources that provided information to the media outlet regarding a criminal corruption case.\textsuperscript{117} Authorities confiscated computers, flash drives, and other journalistic material. Shortly thereafter, a judge charged Germán Sasso, the director of \textit{La Brújula}, with criminal cover-up after he refused to reveal where he obtained leaked recordings related to the corruption case.\textsuperscript{118}

Another case during the previous coverage period also revealed legal harassment against a journalist. In December 2013, Juan Pablo Suarez, the editor of the news website \textit{Última Hora}, was arrested on felony charges of sedition (incitement to public disorder) for filming the arrest of a local police officer in Santiago del Estero. Although he was released after nine days, there was a great deal of criticism surrounding his arrest, as many believed that he had been punished simply for doing his job.\textsuperscript{119} During the arrest, police officers also seized computers and documents from the website's headquarters.\textsuperscript{120}

\textsuperscript{113} Law 26.904, \url{http://bit.ly/1Cto4j}.
\textsuperscript{115} Law 26.388, \url{http://bit.ly/1tg3lpQ}.
\textsuperscript{117} Argentine Forum of Journalism (FOPEA), "Preocupación de FOPEA por allanamiento a La Brújula," [Concern over search at journal La Brújula] October 29, 2014, \url{http://bit.ly/1DakK18}.
\textsuperscript{118} FOPEA, "Repudio de FOPEA al procesamiento del director de La Brújula," [FOPEA repudiates prosecution of La Brújula's Director] November 5, 2014, \url{http://bit.ly/1Daw4do}.
\textsuperscript{119} Committee to Protect Journalists, "Argentina should release editor accused of sedition," December 18, 2013, \url{http://cpj.org/x/5792}; See also: "Liberaron a Juan Pablo Suárez, el periodista santiagueño que estaba detenido por instigar a la sedición," [Juan Pablo Suárez, the journalist accused of sedition, was released] \textit{Infobae}, December 19, 2013, \url{http://bit.ly/1wVPrd}; "Desde Fopea reclaman la libertad del editor Juan Pablo Suárez," [FOPEA Demand the Freedom of Editor Juan Pablo Suárez] \textit{La Noticia} 2, December 17, 2013, \url{http://bit.ly/1G34PvO}.
\textsuperscript{120} Committee to Protect Journalists, "Argentina should release editor accused of sedition."
Surveillance, Privacy, and Anonymity

Although users must provide identification when purchasing a mobile phone or prepaid SIM card, the Argentine government does not impose restrictions on anonymity or encryption for internet users. Bloggers and other online users are not required to register with the government and can post anonymous comments freely in online forums. In March 2014, the Legal and Technical Secretariat issued Resolution 19, a measure which mandates the creation of a section in the Official Bulletin (Boletín Oficial) dedicated to publishing registered domain names, as well as the names of those registering them, which could deter people from applying for domain names.

The National Directorate for Protection of Personal Data issued guidelines for best practices to protect privacy in the development of applications in April 2015. These guidelines establish the obligation of applications and software programs to respect users’ privacy and data protection and outline best practices, such as allowing pseudonyms on applications and creating a transparent privacy policy that provides proper information about the service to the user. Although the guidelines are not binding, they could have a positive impact on users’ privacy.

In general, Argentina upholds high privacy and data protection standards. According to the National Intelligence Law, a court order is necessary to conduct surveillance of private communications, and national intelligence bodies must respect the Personal Data Protection Law when carrying out their functions, meaning, for example, that they have to respect and protect personal data, and no personal information can be disclosed without a judicial order. In 2014, public officials occasionally proposed local initiatives—such as an initiative in the Argentine state of La Plata to monitor social networks for parties and events and thereby “prevent public unrest”—that had the potential to impact users’ privacy and freedom from surveillance. Fortunately none of these initiatives was approved or put into practice.

Argentina does not systematically collect metadata, although a 2013 resolution by the Secretariat of Communications raised some privacy concerns. Resolution 5/2013 regulates the quality of telecommunications services. It states that providers should “guarantee the free access of the CNC [the regulatory body in 2013] to installations… and [should] give them all the information that is required in the set manner and timeframe.” It also establishes a period of three years for service providers to keep all collected data, which will be used to calculate quality indicators. However, the article in question states clearly that the data will be used to calculate quality indicators, and the resolution mentions the obligation to respect personal data. Since its passage in 2013, there has been no evidence to suggest that this provision was implemented in an unlawful or abusive way.

---

Argentina

Although Argentina has legal protections for user privacy, little information is available regarding extralegal or covert surveillance. In mid-2015, the U.S.-based news site The Intercept reported that they had credible evidence that Alberto Nisman and Jorge Lanata, an Argentine journalist, received targeted spyware originating from the same remote domain. Although it is not possible to identify a specific government, agency, or group responsible for the spyware, the targeting of high-profile individuals raises concerns about journalists’ privacy in the country.\(^{128}\)

The government requested data on a number of users in 2014, mostly for the purposes of criminal investigation.\(^{129}\) Between July and December 2014, Yahoo received 155 government requests for data disclosure related to 240 specified Yahoo accounts.\(^{130}\) Out of these requests, Yahoo rejected 22 percent, disclosed only non-content data (basic subscriber information) in 34 percent, disclosed content in 32 percent, and reported no data found in 12 percent.\(^{131}\) During that same period, Facebook, which states that it responds to valid requests relating to criminal cases, received 482 government data requests regarding 708 accounts. Of these, 49 percent of requests resulted in data disclosure.\(^{132}\) Microsoft’s law enforcement requests report for that same period shows Microsoft received 416 requests regarding 512 accounts, of which 2 percent were rejected for not meeting legal requirements and 18 percent, were rejected because no data was found. Of the accepted requests, none of them resulted in disclosure of content, but only non-content (subscriber) data.\(^{133}\)

Intimidation and Violence

The Argentine Forum of Journalism (FOPEA) released its report of attacks on press freedom during 2014.\(^{134}\) According to this report, 178 attacks, ranging from physical aggression to threats to cyber-attacks, were reported during 2014. Digital media outlets reported 13 percent of these attacks, while blogs only accounted for one percent of the attacks.\(^{135}\) These figures represent a slight decrease in comparison with the 194 attacks registered during 2013, eight percent of which were against digital media.

In 2015, two incidents sparked public concern about journalists’ safety and privacy. The first involved the Buenos Aires Herald journalist Damián Pachter. Pachter was the first to report on the death of prosecutor Alberto Nisman—who was investigating a 1994 terrorist bombing and was found dead the night before he was supposed to testify before Congress\(^{136}\)—through his Twitter account\(^{137}\) and


Argentina

later in the *Buenos Aires Herald*. Shortly thereafter, Pachter was informed that he was being surveilled, and had to leave the country immediately.\(^\text{139}\)

After Pachter fled the country, stating that he had no plans to return because he feared for his safety, the national news agency *Télam* published an article online with a screenshot of Pachter’s electronic ticket.\(^\text{140}\) Both *Télam* and the state-run airline Aerolíneas Argentinas have come under criticism for the release of Pachter’s private information and returning flight details. The official twitter account of the Argentine presidential palace, @CasaRosadaAR, retweeted the flight itinerary.\(^\text{141}\) The national news agency and the government argued that they were merely revealing his itinerary to prove that Pachter was not actually leaving the country permanently out of fear; however, critics regarded the incident as a worrisome invasion of a journalist’s privacy.

The search of the offices of the digital media and radio outlet *La Brújula*, and the seizure of evidence and computers from the offices, may also have constituted an instance of harassment (see Prosecutions and Detentions).\(^\text{142}\) FOPEA and the Interamerican Press Society both heavily criticized this search, and the subsequent prosecution of *La Brújula’s* director, after he refused to name his sources relevant to a criminal investigation.\(^\text{143}\) Situations like this could lead journalists to self-censor for fear of being prosecuted or having personal information—or that of their sources—revealed.

**Technical Attacks**

Cybercrime is perceived to be a growing problem in Argentina. Hacker attacks against official government accounts were reported during December 2014.\(^\text{144}\) In 2013, hackers attacked the president’s website and the government’s official Twitter account.\(^\text{145}\)

In December 2014, in the wake of the court-ordered block on the content sharing platform The Pirate Bay (see Blocking and Filtering), hackers attacked the website of the music industry group which sued Pirate Bay.\(^\text{146}\) Also, in November 2014, national news outlet *Clarín*, along with many sites from

---


139 Committee to Protect Journalists, “Journalist flees Argentina after reporting on prosecutor’s death.”


142 FOPEA “Repudio de FOPEA al procesamiento del director de La Brújula.”


other countries, suffered an attack from Syrian hackers. When trying to access the website, the legend “You’ve been hacked by the Syrian Electronic Army (SEA)” appeared.  

The government has created initiatives to combat hacking and cybercrime. For example, the Argentine executive power created the National Program of Critical Infrastructure of Information and Cybersecurity (ICIC) in 2011. This program aims to create a framework to foster identification and protection of strategic infrastructure and is comprised of four working groups, one of which focuses on reducing security breaches and minimizing information safety risks, while another working group offers assessments when emergencies arise as the result of such incidents.

---


Armenia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>28</td>
<td>28</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 3 million
Internet Penetration 2014: 46 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2015 Status: Not Free

Key Developments: June 2014 – May 2015

- In May 2015, an episode of a web series satirizing the police response to protests in Yerevan was removed by YouTube due to a copyrighted clip contained in the video (see Content Removal).
- Proposed amendments to the Law on Personal Data Protection would increase privacy protections by creating an agency with the authority to oversee government decisions with regard to accessing personal data (see Surveillance, Privacy, and Anonymity).
Armenia

Introduction

The internet penetration rate in Armenia has continued improving over the past few years, alongside improvements in the stability of the internet’s infrastructure and relatively few restrictions on online content. Additionally, citizen groups and NGOs have made use of online communication tools to promote and organize campaigns, particularly surrounding the protests in Yerevan against hikes in electricity prices in mid-2015.

While the government generally refrains from blocking or removing online content, in May 2015, an episode of a web series satirizing the police response to protests in Yerevan was removed by YouTube. Allegedly the video was originally flagged by the police for removal, and it was removed due to copyrighted clip in the video. In March 2015, members of parliament proposed amendments to the Law on Personal Data Protection that aim to increase privacy protections by creating an agency with the authority to oversee government decisions with regard to accessing personal data.

Obstacles to Access

Internet access in Armenia continues to grow, although the internet penetration rate remains below 50 percent, and the average access speed was only 3.2 Mbps by the end of 2014. Improvements to the infrastructure have resulted in fewer disruptions to internet service over the past year compared with previous years.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), the internet penetration rate reached 46 percent by the end of 2014, compared with 42 percent in 2013 and just 15 percent in 2009. The Public Service Regulatory Committee of Armenia estimates the rate slightly higher, at 50 percent in 2014.

By the end of 2014, there were approximately 250,000 total broadband subscriptions among the five largest internet service providers, representing an increase of about 23,000 relative to the same period in 2013. The fastest growing ISP is Rostelecom, with 26,208 new subscriptions, an increase by 18,993 subscribers in one year, while Armentel, the largest ISP providing mostly ADSL broadband internet access, is losing ground.

The mobile penetration rate in Armenia was 116 percent as of 2014, and the number of mobile broadband subscriptions is also growing. As of December 2014, broadband subscriptions reached 257,610, an increase of 16,934 compared with of the same period in 2013. The largest mobile internet provider is Orange, followed by VivaCell and Armentel. Based on reports provided by mobile operators, approximately 1.6 million mobile phones out of a total of 3.35 million were connected to

1 International Telecommunication Union, “Percentage of Individuals Using the Internet,” [URL]
2 ARKA Telecom, PSRC 2014 Report, [in Armenian] [URL]
3 Roseltelecom, “Reports,” [URL]; Roseltelecom, Report 2014, [in Armenian] [URL]
5 “Internet usage in Armenia 2014 4Q data stats,” Samvel Martirosyan (blog), April 1, 2015, [URL]
6 Beeline 2014 Report, [URL]
Armenia

the internet as of February 2015. However, according to the Public Services Regulation Commission (PSRC’s) report in 2014, the number of mobile internet subscribers (including mobile 2G and 3G) amounted to 2.1 million out of 3.4 million mobile subscribers, with an increase of over 3 percent increase from the previous year.

All three current mobile operators offer 2G and 3G+ networks, and one operator offers 4G LTE network services. In contrast to the diverse market in Yerevan, the capital city, many villages have only one or two mobile broadband services from which to choose. Approximately 60 percent of rural towns are covered by landline broadband. According to official information from mobile operators, 3G services are available to almost 100 percent of the population, covering 90 percent of the country (excluding mostly unpopulated mountainous regions).

The average monthly price for internet access with speeds of 1 Mbps is around AMD 500 (US$1.00). Many operators are also offering three-in-one packages including IP television and fixed telephone services; the average price for this package with an average speed of 20 Mbps is AMD 10,500 AMD (US$22.00). Prices for broadband internet service vary from AMD 8,000 to AMD 25,000 (US$18 to US$55, respectively), depending on the speed and the quality of services.

Restrictions on Connectivity

There have been no reports of restrictions on internet access imposed by the government or temporary disconnections from the internet since June 2014. In practice, the Armenian government and the telecommunication regulatory authority, the PSRC, do not interfere with or try to influence the planning of network topology. Operators plan and develop their networks without any coordination with either the government or the regulatory authority. Moreover, the regulatory authority requires service providers to indicate any technological restrictions in their public offers. Armenian internet users enjoy access to internet resources without limitation, including peer-to-peer networks, voice and instant messaging services.

Access to the internet in Armenia is ensured through four backbone networks that use fiber-optic cable systems. The international internet connection is made possible by three telecommunication operators. At the network level they are interconnected with fiber-optic cable systems operating in the territory of the Republic of Georgia.

ICT Market

Armenia was one of the first post-Soviet countries to privatize the telecommunication industry. In 1997, the incumbent Armenian operator was sold to a Greek state-owned company with a 13-year monopoly on basic telephone and international data transmission services, including internet. In 2005, the Armenian government revised the incumbent’s license and granted a second GSM license; by 2007, all exclusive rights of the incumbent had been abolished. Since then, Armenian users have been able to choose from three mobile service operators and more than 100 ISPs, though an
analysis of service providers’ official reports shows that the five leading operators together control approximately 90 percent of the market for internet access. The regulatory authorities in Armenia primarily focus on companies with significant market power.

There are 33 companies in the Armenian telecommunications sector providing services including wired and wireless telecommunication services. Within the market for ISPs, 46 percent are foreign-owned companies. Internet service providers offer the following services on the domestic market: ADSL, fiber-optic and cable access, WiFi and WiMax wireless technologies, general packet radio services (GPRS), EDGE, CDMA and 3G technologies (UMTS/WCDMA), 4G LTE. However, internet services based on 4G LTE are available only in limited locations, including Yerevan, Gyumri, Vanadzor, Dilijan, Tsakhkadzor. While the ISP market is relatively diverse, 96 percent of the total revenue from internet service in Armenia is produced by the five largest ISPs, one of which is Armenian, while the other four are foreign-owned.

There are three mobile operators in Armenia: Beeline/Armentel, owned by Vimpelcom, one of the largest mobile operators in Russia (NYSE:VIP), Vivacell-MTS, owned by Mobile TeleSystems, another of the largest mobile operators active in Russia and CIS markets (NYSE:MBT), and Orange Armenia, owned by France Telecom, a leading multinational telecommunications corporation. In 2013, a fourth mobile operator, Ucom, was issued a license allowing its entry into the mobile communications market. Service was expected to start on January 1, 2015, but as of May 2015 it is not yet available.

**Regulatory Bodies**

The concept of an independent regulatory authority was implemented in 2006 with the adoption of the Law on Electronic Communication. Armenia has chosen a multi-sector regulatory model in which there is one body, the PSRC, which is in charge of the regulation of energy, water supply, and telecommunications services. The PSRC’s authority, mechanisms of commissioners’ appointments, and budgeting principles are defined under the Law on State Commission for the Regulation of Public Services.

The members or commissioners of the PSRC are appointed by the president of Armenia and in accordance with the recommendations of the prime minister. Once appointed, a commissioner can be dismissed only if he or she is convicted of a crime, fails to perform his or her professional duties, or violates other restrictions in the law, such as obtaining shares of regulated companies or missing more than five PSRC meetings. The PSRC is accountable to the National Assembly in the form of an annual report, but the parliament merely takes this report into consideration and cannot take any action.

The Law on Electronic Communication contains provisions guaranteeing the transparency of the decision-making procedures of the commission: all decisions are made during open meetings with prior notification and requests for comments from all interested persons posted on the website. However, one of the weakest provisions of the Armenian regulatory framework is the absence of term limits for commissioners: every commissioner can be appointed multiple times, making his or her appointment dependent on current political leaders. In practice, the regulatory bodies in Ar-

---

12 The Law on Public Services Regulation Commission was adopted by the National Assembly of the Republic of Armenia on December 25, 2003.
Armenia

Armenia lack independence due to the strong dependence of the commissioners’ career on political leadership of the country.\textsuperscript{14} For example, in 1995, the broadcasting license of the independent television company A1+ was suspended for refusing to broadcast only pro-government material, and in 2002 its broadcasting frequency was awarded to another company. Despite a ruling by the European Court of Human Rights in 2008, which stated that the regulatory authority’s refusal to reinstate the company’s broadcasting license amounted to a violation of freedom of information, the license was never reinstated.\textsuperscript{15} In September 2012, A1+ began broadcasting on the airwaves of Armnews. During this time, A1+ was nonetheless able to continue publishing news content on its website.

Armenian legislation requires that providers obtain a license for either the provision of internet services or the operation of a telecommunication network.\textsuperscript{16} Procedures for obtaining licenses differ: a service license is obtained through a simplified licensing procedure (purchased for an amount equivalent to approximately US$250), while a network operation license requires verifying the professional and technical capacity of the company and is issued six months after filing the application with the regulatory authority. In 2012, the Armenian government undertook radical reforms of the telecommunication regulatory framework to simplify the market entry procedures of both network operation and services. According to the Amendments to the Law on Electronic Communication, adopted in April 2013, service providers will no longer be required to obtain a license but will simply need to notify the regulatory authority.\textsuperscript{17}

Public access points such as cafes, libraries, schools, universities, and community centers are not required to obtain a license for offering internet access unless they offer services for a fee. In general, according to the licensing law, nonprofit entities are not required to obtain a license for the provision of internet services regardless of their legal status.\textsuperscript{18}

Mobile telecommunication companies are granted a license through regular network operation licensing procedures, but are also required to obtain permission for the use of radio frequencies, which is usually granted through an open auction. An exception can be made if no alternative applicant is interested in a particular frequency, or for frequencies and equipment that do not interfere with other operators’ activities (such as radio relay communication). For cases in which an entity applies for a non-auctioned frequency, the service provider is required to carry out a test for electromagnetic compatibility.

In spite of three well-established ICT-related nonprofit associations, self-regulation of the industry is significantly underdeveloped in Armenia. The oldest nonprofit institution is the Internet Society (ISoc), which is the national chapter of the worldwide ISoc network. At the early stage of internet development in Armenia (1995 through 1998), ISoc Armenia was the primary internet policy advocate and industry promoter. It served as a forum where internet service providers discussed their problems, developed policy agendas, and resolved industry conflicts. However, after the establishment

\begin{itemize}
  \item\textsuperscript{14} There are three independent regulatory authorities in Armenia that are part of the executive, but not a part of the government. These three authorities are the public utilities regulator, the broadcasting regulator, and the competition authority. There is also a civil service commission, which, however, is different from the concept of independent regulatory bodies.
  \item\textsuperscript{17} Law of the Republic of Armenia on Changes and Amendments to the Law on Electronic Communication of April 29, 2013, Official Bulletin No 05/29(969), June 5, 2013.
  \item\textsuperscript{18} Art. 43, Law of the Republic of Armenia on Licensing, of May 30, 2001 with several amendments from 2002-2012.
\end{itemize}
of the independent regulatory authority, ISoc no longer plays as much of a regulatory role, as most industry disputes are filed with the PSRC.

ISoc continues to maintain the registration of domain names, and despite the lack of formal dispute resolution policies, it carries out the registry function effectively with minimal influence from government authorities or the regulator. As a result, the Armenian ICT market enjoys a liberal and non-discriminatory domain name registration regime. ISoc Armenia registers domain names according to ICANN recommendations and best practices. Although members of the ISoc Armenia are individuals, the organization’s board is composed of service provider managers, and in general, the Society’s policy agenda is strongly influenced by the interests of traditional providers that started their business in the mid-1990s.

Another well-established industry association is the Union of Information Technologies Enterprises (UITE). Though industry self-regulation is one of the main goals of the Union, so far it has not developed any significant policies for industry regulation. Both ISoc Armenia and UITE are founders of a third notable nonprofit institution, the ArmEx Foundation, which was established with the sole purpose of creating a local data traffic exchange point. Other founders include leading ISPs, mobile and landline telecommunication operators.

Limits on Content

The Armenian government does not consistently or pervasively block users’ access to content online. In one case, content was restricted in May 2015, when an episode of a web series satirizing the police response to protests in Yerevan was removed by YouTube. The most common incidents of censorship of online content relate to blocking and filtering of platforms and websites by the Russian regulatory authority, which affects access to the same content for some internet users in Armenia, since Armenia receives its web traffic from Russia. However, these cases are promptly resolved by internet service providers once reported by users.

Blocking and Filtering

In general, online content is widely accessible for internet users in Armenia. The most prominent case of online censorship occurred in March 2008 during post-elections events, immediately after clashes between an opposition rally and police resulted in at least eight people killed and hundreds of people injured. The government declared a state of emergency and restricted certain media publications, including independent internet news outlets. The security services demanded that the Armenian domain name registrar suspend the domain names of opposition and independent news sites, and requested that ISPs block certain outside resources, such as some opposition pages on social network platforms, particularly LiveJournal, which was the most popular social network used by opposition and civil society activists for blogging and reporting. Armenian authorities were strongly criticized by international observers for their reaction to the post-election crisis, including the restrictions on access to internet resources. After the events of 2008, Armenian authorities have been

21 Parliamentary Assembly of the Council of Europe, “Observation of the Presidential Election in Armenia,” published April 8,
very cautious about restricting internet content, and no instances of politically-motivated filtering or blocking have been recorded since that time.

Due to the fact that some internet users in Armenia receive filtered traffic from Russian ISPs, there have been a few cases where a website that is blocked in Russia is incidentally blocked for users in Armenia. For example, in May 2015, several gambling websites that had been blocked in Russia by a court decision were blocked in Armenia as well. Following the first reports, Armenian Beeline started to work toward unblocking the websites, which were restored later that same day.

According to Article 11 of the Law on Police, law enforcement authorities have the right to block particular content to prevent criminal activity; in practice, such blocking cases have been limited to locally-hosted, illegal content such as illegal pornography or copyright-infringing materials. For example, in 2012 the police blocked the website Armgirls.am for disseminating pornographic content and for hosting bulletins of women working in the Armenian sex industry. Article 263, section 20 of the criminal code stipulates that the production and dissemination of pornographic materials or items, including printed publications, films and videos, images or other pornographic items, advertisements, or sales is punishable by a fine in the amount of five hundred times the minimum monthly salary in Armenia, or arrest for up to two months or imprisonment for up to two years.

Content Removal

In May 2015, an episode of a web series satirizing the police response to protests in Yerevan was removed by YouTube. Allegedly the video was originally flagged by the police for removal, most likely because it was mocking the police’s behavior and actions, though it was officially removed from YouTube due to copyright infringement, since the video contained a copyrighted clip of a news report.

While currently intermediaries are not liable for the content they host or transmit, in March 2014 members of parliament introduced draft legislation that could establish legal liability for websites that republish or host defamatory comments from anonymous or fake users. Drawing from the European Court of Human Rights ruling in October 2013 that established intermediary liability for third-party comments the proposed legislation aimed to minimize the number of fake accounts on social networks whose defamatory or offensive content is often republished in media outlets. Members of parliament argued that the bill would reduce the frequency with which media outlets reproduce and disseminate slanderous or offensive comments from anonymous users. Critics of this measure, on the other hand, believe it amounts to censorship and that the pressure exerted on media outlets would restrict press freedom. On April 25, 2014, discussions on the draft legislation were postponed for one year, and were later removed from the parliament’s agenda.

Internet service providers involved in transmitting illegal content, such as child pornography, or content related to online crime or cyberterrorism, are not liable for the content they make available

---

Armenia

to their customers, provided that they had no prior knowledge of the content. Any decision of a law enforcement body to block particular content can be challenged in court by the resource or content owners, and if the court rules that the measure was illegal or unnecessary, the resource or content owners may claim compensation. Additionally, Armenia is a signatory to the European Convention on Human Rights; therefore, any such decision can also be challenged at the European Court of Human Rights.

Media, Diversity, and Content Manipulation

Armenian internet users are able to access a wide array of content online, though online media outlets based within the country are subject to financial and political pressures. Currently, self-censorship is not a widespread practice in the online sphere. The Armenian government and the ruling political elite have not applied extralegal measures to prevent political opponents or independent internet resources from publishing online content. However, similar to traditional media outlets such as television or printed press, Armenian internet news resources are exposed to political pressure. In some cases, for example, journalists of a particular online media outlet are not allowed to deviate from the editorial policy of the outlet, which is often linked to one of the political parties. Such pressure has the potential to affect the overall situation of freedom of speech in the country, but it is worth noting that online publishers and individual bloggers strongly resist self-censorship. Indeed, there is a wide diversity of opinion in social media, and virtual battles between supporters and opponents of the government are often observed. A variety of independent and opposition web resources provide Armenian internet audiences with politically neutral, or oppositional opinions.

Digital Activism

There were several significant citizen mobilization movements that occurred in Armenia over the past year that actively used digital media and social platforms for advocacy and to mobilize supporters.

In 2014, changes to the law on temporary disability with respect to maternity leave and temporary disability allowances were met with significant opposition. In the fall of 2014, many stakeholders joined forces to protest the upcoming amendments, which would have based the allowance for maternity and disability leave on the minimum salary and offered commensurate allowances to non-working and working women, with compensation for the latter coming from private employers. The law was passed in December 1, 2014; however, following several debates about the issue online and in the broadcast media, as well as street protests attended by hundreds of pregnant women, the law was amended again in January 2015 to state that working women that receive a salary under AMD 1 million (US$2,000) will be compensated by the state, whereas compensation for women with higher salaries will split between the state and the employer. A Facebook group called “No to Reduced Pregnancy Allowances” played an essential role in raising the issue and mobilizing stakeholders around it.

In late May 2015, another major citizen movement was launched to protest against the increase in electricity prices. A Facebook event was created promoting a rally to protest the price hike, and more than 40,000 Facebook users were recruited via the event page. The first large scale rally took place on May 27. By late June, weeklong street protests were in progress in Armenia’s capital, Yerevan. As a result of the protests, President Sargsyan announced on June 27 that his government would effectively suspend the controversial price hikes, although protests continued into the summer as dem-
onstrators insisted that their demands were not met and continued to condemn the police response to the protests.

**Violations of User Rights**

*There have been few cases of prosecutions against internet users or bloggers for content posted online. While Armenia eliminated criminal penalties for defamation in 2010, concerns over high financial penalties for defamation persist, though the number of cases and the fines have decreased in recent years. Journalists from print and broadcast media have been subject to intimidation and attacks, though no cases of violence against online journalists were recorded during this coverage period.*

**Legal Environment**

Article 27 of the Constitution of the Republic of Armenia guarantees freedom of speech irrespective of the source, person, or place. This constitutional right is applicable to both individuals and media outlets, with some restrictions.

In 2005, Armenian media legislation changed significantly with the adoption of the Law of the Republic of Armenia on Mass Media (also referred to as the Media Law). The most positive changes in Armenian media legislation was the adoption of unified regulation for all types of media content irrespective of the audience, technical means, or dissemination mechanisms. The Television and Radio Law contains additional requirements on content delivery, but it does not regulate news delivery and only addresses the issues of broadcasting erotic or violent programs, as well as the time frame for advertising, the mandatory broadcast of official communications, and rules on election coverage and other political campaigns. Content delivered through a mobile broadcasting platform or the internet is subject to the same regulations.

Armenian criminal legislation grants journalists certain protections related to their profession. According to Article 164 of the criminal code, hindering the legal professional activities of a journalist or forcing a journalist to disseminate information or not to disseminate information is punishable by fines from 50 to 150 times the minimum salary, or correctional labor for up to one year. The same actions committed by an official abusing their position is punishable by correctional labor for up to two years, or imprisonment for the term of up to three years, and a ban on holding certain posts or practicing certain activities for up to three years. However, neither criminal law nor media legislation clearly defines who qualifies as a journalist or whether these rights would apply to online journalists or bloggers.

In May 2010, the Armenian National Assembly passed amendments to the administrative and penal codes to decriminalize defamation, including libel and insult, and introduce the concept of moral damage compensation for public defamation. The initial result was an increase in civil cases of defamation, often with large fines as penalties. In November 2011, the Constitutional Court ruled that...

---

30 Concept of compensation for moral damage caused by defamation was introduced by adding Article 1087.1 to the Civil Code of the Republic of Armenia, Official Bulletin of the Republic of Armenia, 23 June 2010 No 28(762).
Armenia

courts should avoid imposing large fines on media outlets for defamation, resulting in a subsequent decrease in the number of defamation cases. Defamation is widely used by Armenian politicians to restrict public criticism, but it has not necessarily been used to combat oppositional viewpoints or media independence. However, the principle of requiring politicians to be more tolerant of public criticism is not widely adopted in Armenia. According to the Committee to Protect Freedom of Expression (CPFE), in 2013 there were 26 civil defamation and insult suits against journalists (including as a third party) and the media. Of these 26 cases, 17 included media outlets that also have an online presence.

Since 2003, when the concept of cybercrime was first introduced in the Armenian criminal code, criminal prosecution for crimes such as illegal pornography or copyright infringement on the internet demonstrates that Armenian law enforcement authorities generally follow the practices of the European legal system, and neither service providers nor content hosts have been found liable for illegal content stored on or transmitted through their system without their actual knowledge of such content. Armenia is a signatory to the Council of Europe’s Convention on Cybercrime, and further development of Armenian cybercrime legislation has followed the principles declared in the Convention.

Armenian criminal legislation also prohibits the dissemination of expressions calling for racial, national, or religious enmity, as well as calls for the destruction of territorial integrity or the overturning of a legitimate government or constitutional order. Since the Armenian legal system is based on the principle of universality, meaning that laws are applicable online as they are offline, all crimes conducted on the internet are prosecuted similarly to those that are committed offline. Regarding liability for content published on websites hosted in other jurisdictions, Armenian legal theory and practice follows the principle of “place of presence,” meaning that the person is liable if he or she acts within the territory of that country.

Prosecutions and Detentions for Online Activities

No cases of imprisonment or other criminal sanctions or punishments for online activities were recorded over the past year. However, cases of civil liability, such as moral damages compensation for defamation, have been recorded several times over the past few years. The downloading of illegal materials or copyrighted publications is not prosecuted under Armenian legislation unless it is downloaded and stored for further dissemination, and the intention to disseminate must be proved.

Surveillance, Privacy, and Anonymity

On March 4, 2015, the National Assembly approved proposed amendments to the Law on the Protection of Personal Data through the first reading, though as of the end of the report’s coverage period the amendments had not been enacted into law. One key provision within the proposed amendments would create a body that would have the authority to appeal the decisions of state agencies that violate the right to privacy with regard to personal data. The bill provides fines for

31 Cybercrime was defined under the new Criminal Code of the Republic of Armenia, adopted on April 18, 2003. The first prosecution case for the dissemination of illegal pornography via the internet was recorded in 2004.
Armenia

those who violate the law. The amendments are intended to ensure the implementation of the right to personal privacy with respect to the processing of personal data, providing for the harmonization of Armenian legislation regarding personal data with the European standards and international obligations.

The collection of an individual's personal data by the government is allowed only in accordance with a court decision in cases prescribed by the law. The monitoring and storing of customers’ data is illegal unless it is required for the provision of services. Personal data can be accessed by law enforcement bodies only with a court decision. Nonetheless, the courts support most data requests from law enforcement bodies, which usually file motions on data requests while investigating crimes; however, motions must be justified, and if not, the defense attorney may insist on the exclusion of evidence obtained as a result of such action.

Anonymous communication and encryption tools are not prohibited in Armenia; however, the use of proxy servers is not that common due to the fact that since 2008, internet users have not faced problems with website blocking or traffic filtering. Individuals are required to present identification when purchasing a SIM card for mobile phones. No registration is required for bloggers or online media outlets, though tax authorities may question bloggers or media outlets on revenue-related issues (advertisements or paid access).

Armenian legislation does not require access or hosting service providers to monitor transmitted traffic or hosted content. Moreover, the Law on Electronic Communication allows operators and service providers to store only data required for correct billing. Cybercafes and other public access points are not required to identify clients, or to monitor or store their data and traffic information.

Intimidation and Violence

There were no documented cases of violence or intimidation directed at online journalists, however, there have been instances of violence against print or broadcast journalists in Armenia. According to data collected by the Committee to Protect Freedom of Expression (CPFE) in Armenia, in 2014 there were nine known cases of physical violence against journalists.

Technical Attacks

Technical attacks against government websites and civil society groups continue, with most of the attacks originating from the “Anti-Armenia” group based in Azerbaijan.

In addition, Turkish hackers from the Turk Hack Team group claimed that they launched DDoS attacks against websites of the Armenian government, as well as Armenian business and media sites, causing disruptions on April 24, the Armenian Genocide commemoration day. However, there were no interruptions recorded by these entities.

Australia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>17</td>
<td>19</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- New revisions to the Defense Trade Controls Act, passed in April 2015, include restrictions on encryption software that could discourage internet users from taking advantage of such tools for their digital security (see Surveillance, Privacy and Anonymity).

- The National Security Legislation Amendment, passed in October 2014, expands the definition of “computer” to include an entire computer network, which lawyers argue could be misinterpreted to permit surveillance on wide swaths of the internet (see Surveillance, Privacy and Anonymity).

- According to the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015, which came into effect in April 2015, law enforcement and intelligence agencies will no longer require a warrant to access and review metadata, with an exception for the metadata associated with journalists or their sources (see Surveillance, Privacy and Anonymity).
Australia

Introduction

Australians have generally enjoyed affordable, high-quality access to the internet and other digital media, with access continuing to expand over the past few years with the rollout of the alternative National Broadband Network. However 2015 has been a pivotal year for change, with Australia's internet freedom declining slightly from previous years.

The Liberal government, formerly guided in the telecommunications field by Minister of Communications Malcom Turnbull (who became prime minister in September 2015), continues to embrace technology, showing commitment to open up data sets for research and to improve internet connectivity throughout Australia. Under Turnbull's guidance the government continued to roll out an alternative National Broadband Network (NBN), particularly in regional areas that have had poor internet services. The original NBN under the former Labour government was to lay copper cables throughout Australia. The alternative NBN involves a scaled down version using less expensive fiber to the node (FTTN) and was developed after much criticism of the cost and effectiveness of the original NBN plan.1

Recent legislative amendments, however, raised concerns about government surveillance and the potential implications for privacy and freedom of expression. In October 2014, the Australian parliament passed amendments to the national security legislation that increase penalties for whistleblowers and could potentially allow intelligence agents to monitor an entire network with a single warrant. Further, data retention amendments passed in March 2015 require telecommunication companies to store customers' metadata for two years, allowing law enforcement and intelligence agencies to access that metadata without a warrant.2

Obstacles to Access

There are few impediments or obstacles to internet access in Australia. Services continue to improve in remote and rural areas throughout Australia with both the young and elderly embracing connectivity. The ICT sector is mature and competitive with Australians enjoying fair and high-quality internet connectivity.

Availability and Ease of Access

Australia had an internet penetration rate of approximately 85 percent as of December 2014, compared to 83 percent in 2013 and 74 percent in 2009, according to the International Telecommunication Union (ITU).3 The internet penetration rate is expected to steadily increase over the next five years with the implementation of the NBN, which includes expanded wireless, fiber to the node, and satellite services in rural communities. Although internet access is widely available in locations such

as libraries, educational institutions, and cybercafes, Australians predominantly access the internet from home, work, the homes of friends and families, and increasingly through mobile phones.\(^4\)

Access to the internet and other digital media is widespread in Australia. Australians have a number of internet connection options, including ADSL, ADSL 2+, mobile, fixed wireless, cable, satellite, fiber and dial-up.\(^5\) Wireless systems reach 99 percent of the population, while satellite capabilities are able to reach 100 percent.\(^6\) As of December 2014, over 99 percent of internet connections were broadband, while the number of dial-up connections has declined to 159,000 users out of a total of 12.7 million users.\(^7\) Once implemented, the NBN is expected to eliminate the need for any remaining dial-up connections and make high-speed broadband available to Australians in remote and rural areas.\(^8\)

Roughly half of all Australians have access to broadband speeds between 8 Mbps and 24 Mbps.\(^9\) While there are still parts of Australia experiencing slower broadband speeds (approximately 3.3 million people have internet connection speeds of only 1.5 Mbps to 8 Mbps), there has been a steady increase in faster speeds with 2.3 million people connecting to speeds of greater than 24 Mbps.\(^10\) According to Akamai, the average connection speed by the end of 2014 was 7.4 Mbps.\(^11\)

Age is a significant indicator of internet use: 97 percent of Australians between the ages of 15 and 17 are internet users, compared to only 46 percent of those over 65 years old.\(^12\) According to the 2011 Census, 63 percent of Aboriginal and Torres Strait Islanders report having an internet connection, compared with 77 percent of other households.\(^13\) Of those with internet access, 85 percent access the internet through broadband connections.\(^14\) The overall mobile phone penetration rate in Aboriginal communities is unknown.

According to the ITU, there were 31 million mobile phone subscribers in Australia by the end of 2014, compared to 25 million the previous year.\(^15\) Fourth generation (4G) mobile services have driven recent growth, with all networks expanding coverage and experiencing increases in the number of services in operation.\(^16\)

Internet access is affordable for most Australians even though the government no longer subsidizes internet connections for individuals and small businesses in remote and rural areas, where internet affordability is not comparable to that in metropolitan areas.\(^17\) Major internet service providers (ISPs)


\(^7\) ABS, “8153.0 – Internet Activity, Australia, December 2014: Type of Access Connection.”


\(^9\) ABS, “8153.0 – Internet Activity, Australia, December 2014: Type of Access Connection: Advertised Download Speed.”

\(^10\) ABS, “8153.0 – Internet Activity, Australia, December 2014: Type of Access Connection: Advertised Download Speed.”


\(^12\) ABS, “8146.0 - Household Use of Information Technology, Australia, 2012-13: Personal internet use.”


\(^14\) ABS, “Census of Population and Housing: Characteristics of Aboriginal and Torres Strait Islander Australians, 2011.”


such as Telstra also continue to offer financial assistance for internet connections to low-income families.  

Restrictions on Connectivity

There are no limits to the amount of bandwidth that ISPs can supply. While the government does not place restrictions on bandwidth, ISPs are free to adopt internal market practices of traffic shaping. Some Australian ISPs and mobile service providers practice traffic shaping (also known as data shaping) under what are known as fair-use policies. If a customer is a heavy peer-to-peer user, the internet connectivity for those activities will be slowed down to free bandwidth for other applications. Under the iCode, a set of voluntary guidelines for ISPs related to cybersecurity, internet users whose devices have become part of a botnet or who are at high risk of their devices being infected with malware may have their internet service temporarily throttled, or placed in a temporary wall-garden after notification. The ISP supplies the user with information and helps them to clean their devices to become free from botnets and malware. While the aim of the iCode is to improve cybersecurity, in its operation internet connectivity may become temporarily restricted.

ICT Market

Like most other industrialized nations, Australia hosts a competitive market for internet access, with 71 providers as of December 2014, nine of which are very large ISPs (over 100,000 subscribers), another 21 large ISPs (with 10,001 to 100,000 subscribers), and 41 medium ISPs (with 1,001 to 10,000 subscribers). Additionally, there are a number of smaller ISPs that act as “virtual” providers, maintaining only a retail presence and offering end users access through the network facilities of other companies; these providers are carriage service providers and do not require a license. Larger ISPs, which are referred to as carriers, own network infrastructure and are required to obtain a license from the Australian Communications and Media Authority (ACMA) and submit to dispute resolution by the Telecommunications Industry Ombudsman (TIO). Australian ISPs are co-regulated under Schedule 7 of the 1992 Broadcasting Services Act (BSA), meaning there is a combination of regulation by the ACMA and self-regulation by the telecommunications industry. The industry's involvement consists of developing industry standards and codes of practice.
Australia

Regulatory Bodies

The ACMA is the primary regulator for the internet and mobile telephony. Its oversight is generally viewed as fair and independent, though there are some transparency concerns with regard to the classification of content. The ACMA approves self-regulatory "codes" negotiated among members of the Internet Industry Association (IIA). There are over 30 self-regulatory codes that govern and regulate Australian ICTs. In March 2014 the Communications Alliance took over the responsibilities of the IIA through a signed agreement.

Small businesses and residential customers may file complaints about internet, telephone, and mobile-phone services with the TIO, which operates as a free and independent dispute-resolution service.

Limits on Content

There are relatively few limits to online content. However, at times those limits have been the source of controversy for their potential impediment to online freedoms and privacy, such as cases where the attempt to block illegal content online led to the blocking of legitimate content as well.

Blocking and Filtering

Australian law currently does not provide for mandatory blocking or filtering of blogs, chat rooms, or platforms for peer-to-peer file sharing. Websites are blocked or filtered under a narrow set of restrictions. Access to online content is far-reaching, and Australians are able to explore all facets of political and societal discourse, including information about human rights violations. The ability to openly express dissatisfaction with politicians and to criticize government policies is not hindered by the authorities, and complaints may be sent directly to the TIO. However, the legal guidelines and technical practices by which ISPs filter illegal material on websites have raised some concerns in the past years.

Controversy struck in May 2013 when it was revealed that a number of legitimate Australian websites that did not host any type of illegal or even controversial material had been blocked. Investigations revealed that the Australian Security and Investment Commission was using an obscure provision (section 313) of the Telecommunications Act to request the blocking of a fraudulent website. The notice by ASIC to the ISPs specified an IP address that contained the fraudulent website along with a number of legitimate websites, including that of Melbourne Free University. This is the first known incident of ASIC using section 313 to issue notices to ISPs to block non-Interpol material. While access to the affected websites was quickly restored, the use of section 313 in this matter was contentious. This led to a formal review of section 313(3) in 2015 to

29 Telecommunications Industry Ombudsman.
investigate public policy concerns. The committee’s final report was released on June 1, 2015 but has not yet resulted in any new bills or amendments to section 313(3) of the Telecommunications Act.

Web applications like the social-networking sites Facebook and MySpace, the Skype voice-communications system, and the video-sharing site YouTube are neither restricted nor blocked in Australia. Digital media such as blogs, Twitter feeds, Wikipedia pages, and Facebook groups have been harnessed for a wide variety of purposes ranging from elections to campaigns against government corporate activities, to a channel for safety-related alerts where urgent and immediate updates were required.

While the government does not block social media applications within the country, there were some reports in May 2015 that alleged that the Australian government made an informal request for the government of Nauru to block Facebook on the island, though these reports remain unconfirmed. Advocates suspected the Australian government’s involvement due to the fact that Nauru hosts one of Australia’s offshore processing centers for asylum seekers and refugees, and blocking Facebook in Nauru limits refugees in their ability to contact family in Australia. It was reported that the request was made to assist in the Cambodian resettlement policy. UN Special Rapporteur on Freedom of Expression David Kaye also urged the government to revoke the blocking, expressing concern that the measure was “designed to prevent asylum seekers and refugees in the country from sharing information on their situation.”

In March 2015, the Communications Alliance developed the Industry Code Copyright Infringement Scheme, which would require ISPs to issue warnings to users who repeatedly download content illegally (predominantly songs, movies, and TV shows) within a “graduated response scheme” (GRS) where offenders will be warned of their illegal online activity. Unlike GRS systems in other countries such as France and New Zealand, the Australian Scheme does not allow an ISP to terminate an account, apply fines, or throttle those whose activities infringe copyright. As of June 2015, this scheme has not yet been enacted. The Copyright Amendment (Online Infringement) Bill (No 44) 2015, which was passed in June 2015 (outside of this report’s coverage period) will force ISPs to block file-sharing sites such as The Pirate Bay. The bill allows a copyright owner to apply to the Federal Court to order an ISP to block access to a website whose primary purpose is copyright infringement for sites located outside of Australia. It remains uncertain if these measures will be effective, or even enforced.

Australia

Content Removal

There were no cases of the government or other parties forcing content to be removed from websites during the coverage period.

Media, Diversity, and Content Manipulation

The online landscape in Australia is fairly diverse, with content available on a wide array of topics. There are no examples of online content manipulation by the government or partisan interest groups. Journalists, commentators, and ordinary internet users have generally not been subject to censorship so long as their content does not amount to defamation or breach criminal laws, such as those against hate speech or racial vilification. Nevertheless, the need to avoid defamation (and, to a lesser extent, contempt of court) has been a driver of self-censorship by both the media and ordinary users. For example, narrowly written suppression orders are often interpreted by the media in an overly broad fashion so as to avoid contempt of court charges.

Aside from the restrictions on prohibited content, including the incitement of violence, racial vilification, and defamation, Australians have access to a broad choice of online news sources that express diverse, uncensored political and social viewpoints. Individuals are able to use the internet and other technologies as sources of information. Additionally, publicly funded television station SBS features first-rate news programs in multiple languages (available offline and online) to reflect the cultural diversity found in the Australian population.

Digital Activism

Australians use social media to sign petitions to the government, share controversial information, and to mobilize for public protest. Popular protests in 2015 included rallying against the closure of Aboriginal communities in Western Australia, protests against Halal meat and protests at the G20 Summit in Brisbane.

Violations of User Rights

While internet users in Australia are generally free to access and distribute materials online, free speech is limited by a number of legal obstacles, such as broadly applied defamation laws and a lack of codified free speech rights. Additionally, recent amendments have significantly increased the government's capacity for surveillance of ICTs, including an amendment broadening the definition of “computer” to include entire networks, and a provision allowing law enforcement and intelligence agencies warrantless access to metadata.

---

40 Nick Title, “Open Justice – Contempt of Court” (paper presentation, Media Law Conference Proceedings, Faculty of Law, The University of Melbourne, February 2013).
41 Sarah Tallier, “Rallies held to protest against threat of remote community closures in Western Australia,” ABC, May 1, 2015, accessed June 18, 2015. http://ab.co/1YOcoJK
43 Occupy G20 Brisbane, Facebook Community Page, accessed June 18, 2015, http://on.fb.me/1j12qN2
Legal Environment

Australians’ rights to access online content and freely engage in online discussions are based less in law and more in the shared understanding of a fair and free society. Legal protection for free speech is limited to the constitutionally-implied freedom of political communication, which only extends to the limited context of political discourse during an election.44 There is no bill of rights or similar legislative instrument that protects the full range of human rights in Australia, and the courts have less ground to strike down legislation that infringes on civil liberties. Nonetheless, Australians benefit greatly from a culture of freedom of expression and freedom of information, further protected by an independent judiciary. The country is also a signatory to the International Covenant on Civil and Political Rights (ICCPR).

Australian defamation law has been interpreted liberally and is governed by legislation passed by the states as well as common law principles.45 Civil actions over defamation are common and form the main impetus for self-censorship, though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.46 Court costs and the stress associated with defending against suits under Australia’s expansive defamation laws have caused organizations to leave the country and blogs to shut down.47

Under Australian law, a person may bring a defamation case to court based on information posted online by someone in another country, providing that the material is accessible in Australia and that the defamed person enjoys a reputation in Australia. In some cases, this law allows for the possibility of libel tourism, which allows individuals from any country to take up legal cases in Australia because of the more favorable legal environment regarding defamation suits. The right to reputation is generally afforded greater protection in countries like Australia and the United Kingdom than the right of freedom of expression. In Australia this is especially so as freedom of expression is limited to political speech. While the United States and the United Kingdom have recently enacted laws to restrict libel tourism, Australia is not currently considering any such legislation.

Prosecutions and Detentions for Online Activities

In January 2015, a Western Australian court ordered estranged wife Robyn Greewu to pay $12,500 in damages for her defamatory Facebook postings where she alleged that her former husband Miro Dabrowski had emotionally and physically abused her for over 18 years.48 The defence of truth was not proven. This follows the widely publicized earlier decision in the case of Mickle v Farley,49 where a young man in New South Wales was fined AUD 105,000 plus costs for posting defamatory statements on Twitter and Facebook about his music teacher. The case was novel for the amount of damages incurred on the defendant and for being the first Australian decision where a tweet was held to...

be defamatory. In the case Judge Elkaim stated that “when defamatory publications are made on social media it is common knowledge that they spread. They are spread easily by the simple manipulation of mobile phones and computer. Their evil lies in the grapevine effect that stems from the use of this type of communication.”

There have been several cases in the states of New South Wales and Victoria of individuals being sentenced to jail terms for publishing explicit photos of women, typically former girlfriends or boyfriends. By way of example, in 2012 Australian citizen Ravshan Usmanov pled guilty to publishing an indecent article and was originally sentenced to six months of home detention after he posted nude photographs of an ex-girlfriend on Facebook. The sentence was appealed and the court commuted the original sentence in favor of a suspended sentence.

Surveillance, Privacy, and Anonymity

Over the past few years, revelations regarding global surveillance and retention of communications data by the NSA and other intelligence agencies have raised concerns regarding users’ right to privacy and freedom of expression. However, the Australian government has taken few steps to remedy these concerns, and has instead moved to expand the government’s surveillance capabilities. In October 2014, the parliament passed amendments to the national security legislation that increase penalties for whistleblowers and could potentially allow intelligence agents to monitor an entire network with a single warrant. Further, data retention amendments passed in March 2015 require telecommunication companies to store customers’ metadata for two years, allowing agencies to access that metadata without a warrant.

Law enforcement agencies may search and seize computers and compel an ISP to intercept and store data from those suspected of committing a crime. Such actions require a lawful warrant. As will be discussed below, law enforcement no longer requires a warrant to access, review, and store metadata. The collection and monitoring of the content of communication falls within the purview of the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records, however, are regulated by the Telecommunications Act 1997 (TA). It is prohibited for ISPs and similar entities, acting on their own, to monitor and disclose the content of communications without the customer’s consent. Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions. The TIAA and TA explicitly authorize a range of disclosures, including to specified law enforcement and tax agencies, all of which require a warrant. ISPs are currently able to monitor their networks without a warrant for “network protection duties,” such as curtailing malicious software and spam.

50 A 2011 case involving writer and TV personality Marieke Hardy reached a legal settlement in 2012.
Australia

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Bill) is potentially the greatest legislative threat to Australian online freedom. The bill amends the TIAA and TA while introducing a statutory obligation for telecommunication service providers to retain telecommunications data (metadata) for two years. The bill became law on April 13, 2015 and is now referred to as the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (the Act). Telecommunications providers have an 18 month grace period before the applicable provisions enter into force. The metadata of all Australians will be stored for two years. There is no longer the requirement of restricting metadata access and use only in the course of an investigation. Law enforcement and intelligence agencies will no longer require a warrant to access and review metadata. However, law enforcement will still need a warrant to access stored communications, as well as any metadata associated with journalists or their sources.

While other countries have implemented data retention frameworks, the Australian Attorney-General has failed to discuss the significant differences between the EU, American, and Australian legal environments. In other countries, citizens’ rights are protected under a Bill of Rights or a Charter of Human Rights and Freedoms. Like the U.S. courts, European courts can and have struck down data retention laws or directives that offend these guarantees of fundamental human rights and civil liberties. There is no Bill of Rights or Charter of Human Rights and Freedoms in Australia. As such, the courts have no effective means to strike down proposals that violate civil liberties. Once a proposal is enacted, the only way to have it changed is through legislation, which often requires a change of government.

Following the leaks of U.S. National Security Agency documents by former contractor Edward Snowden in June 2013, it was reported that Australian law enforcement has received information from the NSA surveillance programs. It is further believed that the attorney general’s department is seeking the power to “break into anonymization and encryption software like Tor.”

Additionally, in April 2015, new revisions to the Defense Trade Controls Act introduced restrictions on encryption software that could discourage the use of these tools. The new revisions have been criticized for being overly broad, with the potential to criminalize the use of encryption for teaching and research purposes, in addition to everyday use for privacy and security.

The NSA surveillance revelations have further impacted the way in which Australia views its obligations around classified data. On October 1, 2014, the parliament enacted amendments to the National Security Legislation Amendment Act, including provisions that threaten journalists and whistleblowers with a ten year prison term if they publish classified information. These provisions have entered into force. Other worrying provisions that will come into force in 2015 include changes to the scope of warrants. The definition of a “computer” has been broadened to allow law enforcement to access data to multiple computers connected to a network with a single warrant.

Users do not need to register to use the internet, nor are there restrictions placed on anonymous communications. The same cannot be said of mobile phone users, as verified identification

59 National Security Legislation Amendment Act (No. 1) 2014, s 108.
Australia

information is required to purchase any prepaid mobile service. Additional personal information must be provided to the service provider before a phone may be activated. All purchase information is stored while the service remains activated, and it may be accessed by law enforcement and emergency agencies provided there is a valid warrant.60

Intimidation and Violence

There were no reported acts of intimidation or violence resulting from online activities during the reporting period.

Technical Attacks

Cyberattacks and hacking incidents remain a common concern in Australia. Several businesses and universities sustained denial-of-service (DoS) attacks lasting close to a week, disrupting all facets of online university research, teaching, and administration. Private corporations such as those in the mining industry continue to be attacked on a regular basis. The overall rate of cyberattacks has remained steady over the past few years.

Azerbaijan

Internet Freedom Status

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>14</td>
<td>13</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>17</td>
<td>19</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>55</td>
<td>56</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- New regulations restricting media outlets’ and non-governmental organizations’ ability to receive foreign funding has forced some media sites to close down, decreasing the diversity of content online (see Media, Diversity, and Content Manipulation).

- More online activists were arrested on trumped-up charges as the government continued its crackdown against human rights groups, opposition parties, and independent journalists (see Prosecutions and Detentions for Online Activities).

- Self-censorship continues to pervade the online sphere as intimidation rose due to arrests and detentions of online activists and journalists (see Media, Diversity, and Content Manipulation).
Azerbaijan

Introduction

Despite the government’s continued insistence that the internet in Azerbaijan is free and that the authorities do not engage in censorship,¹ there is a stark difference between this characterization and the reality for many internet users in Azerbaijan who have witnessed an increasing crackdown against activism in the country, both online and offline. While the government does not extensively block online content, pro-government trolling continues to distort political discussions, and arrests and intimidation tactics used against netizens and their families over the last few years have threatened online activism. In addition, new amendments to the law on nongovernmental organizations and the law on mass media have made it easier for the government to target critical voices by restricting funding and obtaining court orders to close media outlets.

The crackdown against online activists and journalists became a common practice shortly after 2011 and the Arab Spring. Inspired by the protests around the world, a group of young Azerbaijanis organized protests, using Facebook as their main organizing tool. The repercussions were grave. A number of them were arrested and detained, and police were stationed all across the capital of Baku, monitoring groups of more than five people. Soon after, online activists became clear targets at the hands of the government. This curbing of dissent continued over the course of the coming years, with an unprecedented level of arrests occurring in 2014. A number of prominent journalists, activists, bloggers, civil society activists and human rights defenders were arrested on trumped-up charges. Fearing a spillover of protests from the Euromaidan events in Ukraine, authorities jailed over thirty high profile Azerbaijani citizens between May and December of 2014, some of whom were targeted for their online activism.

Despite these limitations, during this report’s coverage period the internet remained a more open platform for information-sharing and political dissent compared to the independent broadcast or print media outlets, which were forced to shut down or continue their work via their online presence. Facebook continues to serve as an important source of information for Azerbaijani citizens to expose the corruption and the on-going clampdown, particularly as the country prepared to host the inaugural European Games in June 2015.

Obstacles to Access

There has been little improvement to the internet infrastructure in Azerbaijan over the past year, and internet access remains expensive for the majority of the population. The discussions about introducing a countrywide broadband connection and lowering internet costs have led to virtually no results. However, prior instances of communications platforms being blocked by the government, such as the blocking of the image-sharing platform Imgur in 2013, did not occur during this coverage period.

Availability and Ease of Access

Internet access in Azerbaijan continues to expand, while costs and slow speeds remain barriers. Based on the most recent report on the percentage of individuals using the internet released by the ITU, the internet penetration rate in Azerbaijan reached 61 percent by the end of 2014, compared

---

to 59 percent in 2013 and 27 percent in 2009.\textsuperscript{2} A recent World Bank report concluded that the number of high-speed connections (those over 4 Mbps) is less than 10 percent of all connections in the country, with a very small increase in broadband connections over the last two years. According to Akamai, the average internet connection speed in Azerbaijan was 2.7 Mbps in 2014.\textsuperscript{3} As a result, any kind of socioeconomic benefits associated with a higher speed connection such as online job creation, skills development, attracting foreign direct investment, and so on, remain low.\textsuperscript{4}

A government initiative to introduce countrywide broadband internet access by 2017 with speeds in the range of 10-100 Mbps remains on the agenda, with the starting date shifting to 2015 rather than 2014 as originally planned. The total cost of the project is estimated at more than AZN 450 million (US$550 million, before the devaluation of the Manat). To date, there has been little progress in expanding broadband access.

While the Ministry of Communication and High Technologies (MCHT) claims that Azerbaijan leads countries in the region with regard to number of internet users, the country does not perform as well comparatively when it comes to indicators like cost and speed. According to Osman Gunduz, the head of the Azerbaijan Internet Forum, significant milestones were achieved in providing the country with better and cheaper internet; however, in comparison to its neighbors like Russia, Ukraine, Georgia and others, Azerbaijan lags behind not only in providing its users with fast internet but also with keeping costs down. While internet users pay US$25-75 for 4-8 Mbps unlimited ADSL connections in Azerbaijan, in Russia the same speed connection costs only US$7-12. Similarly, the 4-8 Mbps unlimited fiber-optic connection costs US$25-50 in Azerbaijan and only US$8 in Russia. It costs Azerbaijani users US$150 to purchase a 30 Mbps unlimited fiber-optic connection when in Russia the same connection costs only US$12-14. The vast majority of connections in Azerbaijan are based on ADSL, with Wi-Fi, WiMAX, 3G and 4G just starting to become widespread.

A recent World Bank report indicates that while high computer prices are a leading factor in low internet access across the country, mobile phone connections also remain limited. Twenty-nine percent of all households are connected to the internet via mobile phone connections, but further investigation reveals that the average household in Azerbaijan's lower income bracket (lowest 40 percent of the total population by income) needs to allocate 21 percent of their monthly disposable income to afford the cheapest mobile broadband package, and 28 percent of monthly disposable income for the cheapest fixed broadband package.\textsuperscript{5}

Poor telecom infrastructure along with low ICT literacy, expensive computer equipment and high tariffs for satellite connections (owned by the MCHT) remain key obstacles to ensuring greater access across the country.\textsuperscript{6} Adding to the low public awareness is the rural-urban wage gap in Azerbaijan, as well as disparities in fixed telephone coverage. Over 80 percent of all landlines are concentrated in the urban areas, with 47 percent of all fixed landlines located in Baku. This gap has not changed over the last decade. There are parts of the country where only one rural family out of twelve has a telephone line.\textsuperscript{7}

\textsuperscript{5} A Sector Assessment: Accelerating Growth of High-Speed Internet Services in Azerbaijan, 16.
\textsuperscript{7} A Sector Assessment: Accelerating Growth of High-Speed Internet Services in Azerbaijan, 23.
Azerbaijan

Restrictions on Connectivity

There were no cases of intentional disruptions to internet or mobile phone service during the coverage period, although there have been localized government-imposed restrictions in previous years. The Ministry of Communication and High Technologies (MCHT) continues to hold a significant share in a few of the leading ISPs, and the government is authorized to instruct companies to cut internet service under very broadly defined circumstances, including war, emergency situations, and national disasters.8

In the run-up to the presidential election in October 2013, there were reports that several internet cafes were closed down by the Azerbaijani authorities in Azerbaijan’s Autonomous Republic of Nakhchivan. The Institute for Reporters’ Freedom and Safety (IRFS) reported that internet cafes were subject to closure beginning on August 23, 2013. According to the report, internet cafe owners said the MCHT of Nakhchivan issued these orders in an attempt to curb online dissent ahead of the elections. Local residents reported that there is an existing monitoring mechanism and people’s internet activity is closely monitored. In a country with a poor human rights record, restricted political liberties, and with residents living in an information blockade, the shutdown of internet cafes was seen as a calculated decision on behalf of the regional authorities.9

Wholesale access to international gateways is maintained by companies with close ties to the government. Only two operators in Azerbaijan are licensed to connect international IP traffic: AzerTelecom and Delta Telecom. Delta Telecom is the main distributor of traffic to other ISPs and is also a transit operator of Azerbaijan’s segment of the Europe Persia Express Gateway (EPEC). Delta Telecom owns the country’s internet backbone and has external fiber-optic connections with Russia (via TransTelecom) and with Turkey (via RosTelecom). It also controls the only Internet Exchange Point (IXP) in Azerbaijan and charges the same amount for local and international traffic. The second licensed operator, AzerTelecom, has a fiber-optic cable network covering all major regions in Azerbaijan, including the autonomous republic of Nakhchivan.

ICT Market

The ICT market in Azerbaijan is fairly concentrated: Delta Telecom (previously AzerStat) maintains the largest share of the market, bringing about 99 percent of internet traffic into the country. In addition, it sells traffic to over 30 ISPs, including three state-owned providers: AzTelekomnet (Azertelecom), BakInternet and Azdatakom.10 It was the first company to implement a WiMAX technology project in February 2010, laying the foundation for the use of wireless, broadband, and unlimited internet access. The largest ISP operating outside of Baku is the state-owned Azertelecom, with ownership ties to the MCHT and whose shareholders include Azerfon, which has links to the president’s daughters.11

8 According to clause 4.2(a) of the “Rules for Using Internet Services,” internet providers can unilaterally suspend services provided to subscribers in cases that violate the rules stipulated in the law “On Telecommunications.” Furthermore, a provider can suspend the delivery of internet services in certain circumstances including in times of war, events of natural disasters, and states of emergency; though none of these legal provisions were employed in 2013-2014. See, The Expression Online Initiative, Searching for Freedom: Online Expression in Azerbaijan, November 2012, http://bit.ly/1Oai45j.
Azerbaijan

Azertelecom completed its fiber-optic network in 2011 and is now competing for Delta Telecom’s business. More recently, Azertelecom’s revenues have dipped as Azerbaijani users are increasingly turning to Skype or other Voice over Internet Protocol (VoIP) services for cheaper phone calls.

Despite the fact that over 30 ISPs operate in the country, the state-owned companies control over 56 percent of the market share. The market base is split along geographical lines. AzTelekomnet (the former Aztelekom) serves the Azerbaijan regions, and BTRIB (Baku Telephone Production Association) serves the capital.

The country’s fixed broadband market is still in its emerging phase. There exists little equality in particular between operators. The lack of regulatory reform also inhibits development of the sector. Government control, high internet prices, and the influence of the Ministry of Communications and High Technologies (MCHT) over two of the largest operating companies are concerns for local and foreign investors.

Regulatory Bodies

The government of Azerbaijan continues to play a leading role in regulating the market, both through the state-owned companies and through government institutions. All internet service providers are regulated by the Ministry of Communication and High Technologies (MCHT, formerly the Ministry of Communication and Information Technologies), which lacks independence. The MCHT is responsible for establishing and enforcing policies related to the ICT sector, and reports to the government on how much financial support should be allocated for the sector.

Limits on Content

The government has yet to implement systematic or widespread blocking or filtering of websites or social networks. YouTube, Facebook, Twitter and international blog-hosting services are freely available. However, the government continues to resort to other measures to limit freedom of expression online, particularly the intimidation and arrest of internet users on trumped-up charges leading to self-censorship (see Violations of User Rights). Over the past year, the government has also ramped up economic pressures, such as regulations restricting foreign funding and donations to organizations in Azerbaijan, effectively cutting off funding to a number of media outlets.

Blocking and Filtering

The government does not engage in extensive blocking or filtering of online content, instead relying primarily on legal, economic, and social pressures to discourage critical media coverage or political activism. Websites that have been blocked in the past include satirical websites, petitions, and other content criticizing the government. Over the past few years, blocked websites have included Eqreb, a satirical website originally blocked in 2010; Tinsobeti, a website that “offered a mix of straight poli-

---

14 A Sector Assessment: Accelerating Growth of High-Speed Internet Services in Azerbaijan, 19.
Azerbaijan

Critical commentary and a good dose of caricature, usually of the President Aliyev,16 which was blocked in 2005 shortly after it began publishing; and Susmayaq.biz, an online petition calling for a reduction in energy prices, which was blocked shortly after it began operating in 2007. Access to these websites today is no longer possible as their domains have expired.

There is still no established process through which affected entities can appeal in cases where opposition websites or other materials have been blocked, and there is still no information on the total number of blocked websites in Azerbaijan. Decisions to block online content are not transparent, and when users try to access blocked websites they simply receive an error message, rather than information stating that the site has been blocked. There is no law that includes an exact definition of what stipulates the reasons for blocking or shutting down websites.

Content Removal

In addition to sporadically blocking websites, the government has succeeded in removing several social media pages that produce political satire or are otherwise critical of the Aliyev government. In general, authorities rely on pressure and threats (rather than court orders or other takedown procedures) to remove unwanted content: some activists who are administrators of social media websites targeted by the government have subsequently deleted their pages after having been arrested or detained for questioning.

There are few examples of forced deletions of online content based on a takedown notice system, and these cases are primarily related to personal data. Subject to Articles 5.7 and 7.2 of the law “On Personal Data,” personal data published without the consent of an individual must be removed from websites following a written demand from the individual concerned, a court, or the executive branch. The personal data law regulates the collection, processing, and protection of personal data (name, surname, patronymic, date of birth, racial or ethnic background, religion, family, health and criminal record), the formation of the section of personal data in the national information space, as well as issues related to the cross-border transfer of personal data to define the rights and obligations of public bodies and local authorities, individuals, and legal entities operating in this area.17 Additionally, both the MCHT and the Ministry of Education run a hotline program to uncover allegedly illegal and dangerous content.18

Media, Diversity, and Content Manipulation

The ongoing government crackdown against independent and opposition media outlets—in addition to arrests of online activists over the past few years—has significantly limited the space for free expression in Azerbaijan. Some online journalists, commentators, and ordinary internet users have resorted to self-censorship, especially if they are employed by state media outlets or progovernment platforms. Netizens are fully aware of the consequences of expressing controversial online opinions. The growing environment of fear has pushed many individuals online and offline to either keep their thoughts to themselves or limit their opinions to non-political issues.

Azerbaijan

To counter longstanding restrictions on media freedom, alternative online platforms emerged and expanded beginning in 2005, and the Azerbaijani blogosphere blossomed in subsequent years. Blogs critical of the government gained popularity following the 2008 presidential elections. Local BarCamps (user-generated technology conferences) and the introduction of Azerbaijani language blogging platforms also helped create alternative spaces of information on many subjects ignored or distorted by traditional media. The impact and importance of a free and open internet has become even more vital in the past year with the closure of remaining independent media outlets like the Radio Free Europe/Radio Liberty’s Azerbaijani service and the blocking of foreign funding to the local non-governmental organizations and media outlets. However, the ability for online bloggers and activists to produce and disseminate controversial content online is threatened by government pressure, thus limiting the diversity of content available in the online sphere.

The limits imposed on independent or opposition media outlets make it extremely difficult for them to maintain enough stable advertising to sustain the platform. Often, large businesses and companies shy away from working with these outlets for the fear of losing their business license or receiving other unwanted pressure from the government.

Additionally, new amendments regulating the foreign funding of NGOs have made it easier for the government to target local organizations and media outlets that receive grants from outside sources. In February 2014, President Aliyev approved amendments to the law on grants, further restricting the space for the civil society operations. Further, in February 2015, Aliyev signed amendments to the mass media law that allow the courts to order the closure of any media outlets that receive foreign funding or that are convicted of defamation twice in one year. The complicated new requirements for receiving grants prevented a number of online media outlets from continuing their work. Outlets such as Mediaforum.az, Obyektiv TV, Channel 13, and Zerkalo/Ayna all had to cease operations in light of the new restrictions.

The vast majority of existing online media outlets publish news in favor of the government. Although there is no direct influence by the government over these platforms, the owners and managers of these outlets dictate the content, making sure no content is critical toward the government or government policies. Often, media owners have strong ties to the government or are affiliated with some high-ranking official within the government.

Online trolling continues to be a problem in Azerbaijan and has become more extensive and more coordinated over the last five years. Research into pro-government trolling in Azerbaijan notes the increase in intensity and coordination of responses, suggesting that the government has moved from viewing the online sphere with apathy toward adopting a policy of actively manipulating online discussions.

In advance of the launch of the European Games, which were held in Azerbaijan in June 2015, international criticism of the country’s rights record grew. While nearly all progovernment media outlets were actively engaged in refuting any claims about the country’s deteriorating human rights record, a group of progovernment youth was deployed to troll international media outlets and foreign and local critics in online spaces, particularly on Twitter. These trolls and bots refuted any antigovernment and anti-Aliyev articles, comments, and statements online, often using violent or degrading

---

Azerbaijan

language. A brief look at the profiles of these Twitter users showed some of them were students of the Baku State University, Azerbaijani Diplomatic Academy, University of Languages, and Slavic University. Others were members of such progovernment youth movements as AGAT (Integration of Azerbaijani Youth to Europe) and the youth branch of the ruling party, Yeni Azerbaijan.

Digital Activism

Despite the shrinking space for independent media online and the crackdown against online activists over the past two years, activists continue to use social media platforms to disseminate information and organize campaigns, though the impact is fairly limited.

The most popular online campaign during the report’s coverage period was organized shortly after a deadly fire in the capital of Baku that killed 15 people. On May 19, 2015, a fire ripped through a 16-story apartment building due to the poor quality of the building’s external cover. Over 200 buildings are covered with the same poor quality external cover as a result of a mass beautification attempt by the city administrative office. The campaign “#oYanaq” (“let’s wake up”) was created and used widely to call on the government to take responsibility for the fire and the deaths of innocent residents, as well as to demand the tearing down of all other similar covers. The discussions on Facebook between angry and frustrated residents of Baku prompted emergency meetings on the government level; however, many buildings around the capital remained covered and as of the end of May, the local authorities were yet to finalize the removal of the covers.

Additionally, in the run-up to the European Games, a Facebook page was started called “Refuse being a volunteer at the European Games,”21 a new campaign drawing attention to the corruption behind the upcoming event, and exposing the ongoing crackdown. While it generated much attention, especially among university students who were forced to volunteer in return for grades and exam passes, it did not lead to significant protests. It is likely they were afraid of losing their spots in school or feared repercussions from participating in such a protest action. Nevertheless, given the limited space for gathering and association, this campaign was regarded as a positive development, especially among young men and women in Azerbaijan.

Another popular social media campaign was developed following the death of a young woman Aytac Babayeva, who was brutally stabbed in broad daylight. Her death prompted discussions about violence against women, a taboo topic in Azerbaijan. The hashtags #AytacBabayeva and #AytacBabayevaOlumsuzdur (“Aytac Babayeva is Eternal”) were widely used to draw attention to her death and the death of many other women who face violence on a daily basis. A number of community pages were launched on Facebook, each gathering thousands of “likes”.

Violations of User Rights

The Azerbaijan government continues to arrest and harass internet users as a means of stifling dissent and activism. A number of online activists have been arrested over the past few years, in particular young activists and journalists who post information and opinions critical of the government. Government surveillance and monitoring of social media accounts continues be an issue: many activists and

opposition party members who are arrested or detained report that police have referenced their online communications during interrogations.

Legal Environment

While the right to freedom of expression is guaranteed in the constitution and Azerbaijan is a signatory to binding international agreements, including the International Covenant for Civil and Political Rights and the European Convention on Human Rights, the Azerbaijani government frequently fails to protect the right to freedom of expression, both offline and online.

Libel is the most common criminal charge used by the authorities against journalists in Azerbaijan. While the online sphere was previously considered a form of mass media and was regulated under the Law on Mass Media, as of May 14, 2013, defamation committed online is prosecutable under the criminal code. With the new amendments, online defamation is now punishable by up to six months in prison, or up to three years in prison in cases of aggravated defamation. In a further move, one likely to curb free speech and intimidate activists, the same amendments increased the maximum sentence for “administrative arrests” from 15 days to three months. Administrative arrests, under charges such as disorderly conduct, have been used to target activists and journalists over the past few years.

Prosecutions and Detentions for Online Activities

Online activists and journalists are most often prosecuted based on trumped up charges, including drug possession, hooliganism, and more recently, treason, tax evasion, abuse of authority and embezzlement. A number of website administrators and bloggers in Azerbaijan are in jail for their online activities, including Abdul Abilov, who ran a website called “Let's Say Stop to Toadies,” Omar Mammadov, who created a satirical site called “Snippets from Azerbaijani TV,” Faraj Karimov, whose site was called “Resign,” and others. In some cases, authorities have also gone after family members of activists. The father of Zohrab Hasanov, an Azerbaijani activist living in Germany, was summoned for questioning by the police on March 14. Hasanov is creator of a Facebook page titled “Azerbaijan without dictatorship.” A number of editors-in-chief of online news outlets remain in jail, including Nijat Aliyev and Sardar Alibeyli.

Other activists and journalists were arrested or sentenced during the coverage period for their online activities:

- On January 27, 2014, Omar Mammadov, a 19-year-old cofounder of the youth movement Axin (“the Current”) was detained and charged with illegal drug possession. Mammadov was using his personal Facebook page to criticize the authorities. An active blogger, Mammadov is also a former administrator of a satirical Facebook page “Snippets from Azerbaijani

---

26 Dikturasiz Azəbaycan, Aserbaidschan ohne Diktatur, Facebook Community Page, https://goo.gl/0cpSLR.
Azerbaijan

TV, with some 57,000 followers. On July 4, 2014, Mammadov was sentenced to five years in prison.

- Two brothers, Faraj and Sirac Karimov, were arrested a week apart in July 2014. Both are members of the opposition Musavat party. Faraj was an administrator of a popular Facebook page called "Istefa" ("Resign") which he created in the run-up to the presidential elections. Sirac Karimov was arrested by mistake instead of his brother a week prior. Despite the fact that the police recognized this mistake, they kept Sirac jailed. On March 16, 2015, Sirac was sentenced to six years on drug possession charges. Faraj was sentenced to six and a half years on May 6, 2015. Both were charged under Article 234 of the Criminal Code (illegal possession and sale of drugs), even though during their interrogations the police questioned them about their political activism, specifically asking Faraj about the Facebook pages he administered. Both brothers denied the charges of illegal drug possession, saying their arrest and sentence was the result of their activism and political views.

- Mehman Huseynov, a young activist, blogger, and photojournalist, was arrested on October 27, 2014, and taken to the Investigation Department of the Prosecutor General for Serious Crimes where he was questioned about his political satire website, and about his brother, Emin Huseynov, who is the former director of the Institute for Reporters Safety and Freedom. He was prevented from leaving the country on November 10 while he was on his way to an OSCE conference in Tbilisi. Emin Huseynov is currently in hiding at the Swiss Consulate in Azerbaijan since August due to government persecution, and was formerly the director of the Institute for Reporter’s Freedom and Safety. Mehman Huseynov was detained again on November 29 when all of his documents (passport and national ID) were taken away from him. He currently has no documents, cannot leave the country and is facing criminal charge for hooliganism and resisting police in an ongoing investigation.

Surveillance, Privacy, and Anonymity

It is unclear to what extent security agencies monitor ICT activity or track user data in Azerbaijan, though the experience of activists and bloggers who are detained by the authorities points to a high likelihood that the government is engaging in extensive online surveillance. Most internet users do not have licenses for the software on their computers, which leaves them vulnerable to security threats such as viruses and other malicious programs that could be implanted to monitor their activity. While the law explicitly prohibits the arbitrary invasion of privacy, and court orders are required for the surveillance of private communications, the law “On Operative-Search Activity” (Article 10, Section IV) authorizes law enforcement agencies to conduct surveillance without a court order in cases regarded as necessary “to prevent serious crimes against the person or especially dangerous crimes against the state.” The unclear parameters for what constitutes preventive action leave the law open to abuse. As such, it has long been believed that the Ministry of National Security and Ministry of Internal Affairs monitor the phone and internet communications of certain individuals, especially foreigners, known activists, and business figures.

In February 2014, Citizen Lab reported that Azerbaijan, along with 20 other governments, is suspected of using RCS (Remote Control System) spyware sold by the Milan-based company Hacking

---

Azerbaijan

Team.\textsuperscript{28} RCS spyware allows anyone with access to activate a computer’s webcam and microphone and steal videos, documents, contact lists, emails, or photos from that particular computer. The spyware has been used in the past by the Moroccan government to spy on the media outlet 

\textit{Mam-fakinch}, by UAE authorities to spy on human rights activist Ahmed Mansoor, and more recently was used to target Ethiopian journalists in Washington, D.C.\textsuperscript{29} In July 2015, leaked documents from the intelligence technology and surveillance company Hacking Team revealed that the government of Azerbaijan was also a client.

In December 2011, the Cabinet of Ministers endorsed a plan—without parliamentary approval—that would require registration for all mobile devices. The plan requires the registration of IMEI codes (the unique serial number given to each phone), SIM cards, and mobile network numbers. Unregistered devices are listed on a “black page,” and mobile service providers are required to limit service to all devices under this category. The registration process began on March 15, 2013, and a statement from the Deputy Minister of Communication and Information Technologies indicated that service would be affected for phones on the “black page” beginning May 1, 2013. More than 13 million mobile phones are currently registered under the new system.

In August 2014, following escalations on the border with Armenia, Member of Parliament Siyavush Novruzov suggested introducing a requirement for users to register on social media and other websites under their own names to avoid “insulting and abusive language” used by people “writing under pseudonyms.”\textsuperscript{30} Novruzov said users would register using their national IDs, claiming this method was already in use in many other foreign countries. Independent observers in Azerbaijan decried this proposal as an infringement on freedom of expression, especially as anonymity is becoming an integral part of debate online. To date, no further attempts have been made in this direction by the authorities following the statement.

\textbf{Intimidation and Violence}

Physical attacks and violence against internet users became more common since the 2009 case of the “donkey bloggers,” when Emin Milli and Adnan Hajizada—two youth activists and founders of popular youth networks—were assaulted at a restaurant in downtown Baku shortly after posting a video that went viral mocking the government of Azerbaijan. The two men were beaten and later arrested and charged with hooliganism.

Most harassment against online activists manifests in the form of arrests, detentions, and interrogations. The government of Azerbaijan also uses travel bans against activists and human rights defenders, as well as members of non-governmental organizations. For example, as previously noted, online activist Mehman Huseynov has his passport and his national ID card taken away from him without any further explanation, and he was prevented from leaving the country. Mehman’s brother, Emin Huseynov, who is the former director of IRFS, has been in hiding at the Swiss Embassy in Baku since August 2014 due to harassment from the government and the threat of prosecution.

\textsuperscript{29} Ibid.
Azerbaijan

Technical Attacks

A number of opposition news websites continue to be subject to cyberattacks, resulting in temporary shutdowns. These include the news websites Yeni Musavat, Azadlıq and the Radio Free Europe/Radio Liberty local service, Azadlıq Radiosu. The majority of attacks occurred during politically sensitive events, such as elections.31 As a result, opposition papers subject to attack have speculated that the cyberattacks were launched by the Ministry of Defense. The ministry, however, denies these allegations.32

On December 10, 2014, AzNet announced that the American company Arbor Networks—a security solutions provider for network operators and large corporations—would provide network protection for AzNet due to ongoing attacks and, more recently, DDoS attacks of 85 Gbps capacity on the network of mobile operators in Azerbaijan. DeltaTelecom also announced its decision to sign up for an additional protection against DDoS attacks.33

Between January and February 2015, Mia.az, an online pro-government news platform, reported that its website was subject to hacking attacks and was therefore experiencing temporary issues in staying online, forcing the website to close for a short time before reopening. Its editors and management said the attacks took place shortly after the platform published pro-Aliyev articles.

Bahrain

Key Developments: June 2014 – May 2015

- News emerged in April 2015 of plans to create a Bahraini national search engine that would allow authorities to easily filter unwanted search results without the need to secure cooperation from U.S.-based companies. The project is reportedly being done in collaboration with Russian experts behind that country’s "Sputnik" search engine (see Blocking and Filtering).

- At least three popular Twitter users were pressured into deleting their tweets or closing their accounts for posts that were critical of government policy. Around 97,000 tweets were erased from the satirical account @Takrooz after he was arrested, leaving only one tweet in place stating, “They tortured me in prison” (see Content Removal).

- The Ministry of Interior warned users against making any statements that were critical of Bahrain’s role in supporting the Saudi-led coalition that conducted airstrikes in Yemen (see Media, Diversity, and Content Manipulation).

- Several users, including a former member of parliament, were prosecuted for calling for a boycott or exposing unfair practices in the lead up to November 2014 parliamentary elections. At least 11 users were arrested for posts that were critical of King Abdullah of Saudi Arabia after his death in January, including two teenage girls. Four young men were each sentenced to three months in prison for “offending in public a foreign country or its president or representative” (see Prosecutions and Detentions for Online Activities).

- Well known human rights activist Nabeel Rajab, who has faced legal harassment for several years, was arrested twice over the coverage period for Twitter posts critical of the Bahraini security forces, the Saudi-led airstrikes in Yemen, and the alleged torture of detainees at Jaw prison (see Prosecutions and Detentions for Online Activities).

- A computer crimes law was passed in December 2014 that, among other things, criminalizes the encryption of data if done with “criminal intentions” (see Surveillance, Privacy, and Anonymity).
Introduction

The internet, currently the last remaining ground for free expression seekers in Bahrain, continued to fall victim to tight surveillance and restrictions on speech in 2014-2015. Whether tweeting under nicknames or real names, users faced arrest, prosecution, and often mistreatment at the hands of security forces for everything from serious government criticism to satirical jokes about the late Saudi king. At least 27 users were arrested, detained, or prosecuted over the coverage period. While the majority of users are still on trial, 11 Bahraini users were collectively sentenced to 29 months of prison, while 12 continue to languish in prison as a result of harsh sentences passed in previous years. Bahraini law does not contain adequate protections for free speech, given provisions that ban criticism of the royal family, the spreading of false news during war, or insulting the foreign politicians. A computer crimes law passed in December 2014 contains several standard punishments for illegal wiretapping communications or hacking computer systems, but also criminalizes the access or possession of online electronic pornography as well as the use of encryption for “criminal purposes.” The broad wording of the latter provision has worried activists who depend on encryption tools to document human rights abuses and to speak freely about political affairs, activities that are routinely considered criminal acts in the country.

In an alarming development, several Twitter users were coerced into deleting thousands of tweets or closing their accounts altogether. In June 2014, around 97,000 tweets were apparently erased from the well-known account of the satirical Twitter user “@Takrooz” after he was arrested. Only one tweet remained on the account, stating, “They tortured me in prison.” In September 2014, government critic Ghada Jamsheer was forced to close her account after she was detained for several weeks. YouTube videos also faced censorship for containing content showing government officials in a negative light. In July 2014, a YouTube video in which an exiled activist accused the Bahraini chief of public security and an Interior Ministry spokesperson of human rights abuses while speaking with them in Geneva was taken down on alleged copyright grounds after gaining 83,000 views. It was later reinstated within a few days after the matter was resolved with Google, YouTube’s parent company.

In the absence of a representative government, many Bahrainis continue to look to the internet as an outlet for expressing political, economic, and social frustrations in the country. Crackdowns on Bahraini internet users escalated in 2011, following widespread protests against the ruling family of King Hamad bin Isa al-Khalifa. The authorities engaged in mass arrests, military trials, torture, and widespread intimidation tactics in an attempt to silence popular demands for greater political rights and democratic freedoms, including a new constitution and an elected government. One online activist died from torture while in police custody in April 2011, and the court failed to hold anyone accountable for it, amid a culture of impunity. Unfortunately, as the importance of online tools has grown, so too has the desire of the Bahraini authorities to extend censorship and government repression practices from the real world into the online domain.

Obstacles to Access

From a technological perspective, Bahrain is one of the most highly connected countries in the world. Competitive broadband prices have led to high levels of mobile internet penetration. However, the market for service providers is not free, with all providers de facto controlled by a government agency able to order restrictions on access and certain content at will.

Availability and Ease of Access

In 2014, Bahrain ranked first in the Arab region in the International Telecommunication Union’s (ITU) Information and Communications Technology Development Index. Internet access is widely available at schools, universities, shopping malls, and coffee shops, where Bahrainis often gather for work and study. Language is not an issue, with adult literacy at nearly 95 percent. Bahrainis also possess a high level of English language proficiency, and many ICT applications are available in Arabic. The government provides free computer training programs, which have served 13,300 citizens as of August 2014. The number of internet users has risen rapidly, from a penetration rate of 33 percent in 2007 to 91 percent in 2014. Bahrain also has one of the highest mobile phone penetration rates in the region at 173 percent as of the end of 2014, representing over 2.3 million subscribers.

As of the third quarter of 2014, there were approximately 1.8 million broadband subscriptions in the country, of which 91 percent were mobile broadband. Dial-up connections disappeared in 2010, and ADSL use has declined with the growth of mobile broadband. 4G LTE has been available since September 2013. Prices for mobile broadband and are among the lowest in the region, where a subscription for 5GB of data on a 4G LTE network is available for USD 16 monthly. However, prices are still high for residential high speed broadband in comparison to countries in the Organization for Economic Cooperation and Development (OECD). Average peak connection speeds have declined over the third quarter of 2014 to 22.7 Mbps.

Restrictions on Connectivity

Although there is no centralized internet backbone in Bahrain, all ISPs are indirectly controlled by the government through orders from the Telecommunications Regulation Authority (TRA). This tight control over the country’s ICT sector has allowed the Bahraini authorities to enforce strict limits on online content. For example, the authorities have occasionally throttled internet speeds around certain events, such as the anniversary of the February 14 protests, in previous years.

---

9 TRA, Telecommunications Market Indicators in the Kingdom of Bahrain, slide 39.
11 TRA, Telecommunications Market Indicators in the Kingdom of Bahrain, slide 40.
12 Akamai, State of the Internet Report, Q3, Volume 8 number 3, September 2014 http://akamai.me/1Bfgac3.
Bahrain

In June 2013, the Minister of State for Communications announced that Bahrain would introduce new regulations for Voice over Internet Protocol (VoIP) applications, such as Skype, WhatsApp, Viber and Tango, currently popular in Bahrain. Authorities stated the move was made for “security considerations” and to preserve moral values.13 As of mid-2015, no action had yet been taken on the issue.

ICT Market

Batelco, Zain, and VIVA are the three mobile phone operators in the country, and also serve as its main internet services providers (ISPs). The government has a controlling stake in Batelco, the largest of the three, while other ISPs are owned by investors from the private sector, including non-Bahraini investors.

Regulatory Bodies

Mobile phone services and ISPs are regulated by the Telecommunications Regulation Authority (TRA) under the 2002 Telecommunications Law. The TRA is responsible for licensing telecommunication providers and for developing “a competition led market for the provision of innovative communications services, available to all.”14 Although the TRA is theoretically an independent organization, in practice its members are appointed by the government, and its chairman reports to the Minister of State for Telecommunications. Until June 2013, this minister also occupied the post of President of the Information Affairs Authority (IAA).15 The IAA, which replaced the Ministry of Information in 2010, oversees both traditional and online media outlets in Bahrain and is responsible for decisions to block websites, which are then enforced by internet service providers (ISPs).

There have been no reported instances of ISPs being denied registration permits. Indeed, over 31 licenses have been granted since 2003, with 14 providers currently in business.16 However, in early 2015 the TRA revoked the licenses of 14 small ICT companies, including some that voluntarily requested the cancellation. According to observers, the majority of these companies were offering international calling services that were adversely impacted by the growing use of Voice over IP (VoIP) applications, leading many to bankruptcy.17 While the official reason for the license cancellations was not made public, TRA mentioned that the order was in accordance with Article 35 of the Telecommunications Law,18 which permits license revocation in cases of “material breach of any provision of this Law” or “serious indications or evidence that a Licensee is likely to commit such breach,” and if the licensee failed to comply with TRA’s directions.19 The head of TRA said that the number of small companies in the telecommunication market would be reduced by 50 percent.20

---

15 In June 2013, Mohamed al-Rumaihi was named President of the IAA, replacing Fawaz al-Khalifa who remained Minister of State for Telecom.
16 TRA, Telecommunications Market Indicators in the Kingdom of Bahrain, slide 7.
Bahrain

Limits on Content

The level and sophistication of censorship remained stable over the past year, with the government continuing its efforts to silence online dissidents by forcing them to close their pages or remove content. Self-censorship is rife, particularly on issues related to the monarchy, religion, and relations with the neighboring countries of the Arabian Peninsula. Despite these limitations, many still turn to the internet to collect independent information and to call attention to gross human rights violations.

Blocking and Filtering

The Bahraini government engages in extensive blocking of online content. Multiple state organizations, including the IAA, the Ministry of Interior, and the Ministry of State for Telecommunication, can order the blocking of a website without a court order. The IAA blocks websites that violate Articles 19 and 20 of the country’s Press Rules and Regulations, which include material judged as “instigating hatred of the political regime, encroaching on the state’s official religion, breaching ethics, encroaching on religions and jeopardizing public peace or raising issues whose publication is prohibited by the provisions of this law.”21 Thus, any site that criticizes the government, the ruling family, or the country’s status quo is subject to blocking by the IAA. In a new development, news emerged in April 2015 of plans to create a Bahraini national search engine with the help of Russian technology experts, based on Russia’s “Sputnik” search engine. This could enable the Bahraini authorities to easily filter unwanted search results without the need to secure cooperation from U.S. based search engine companies, such as Google.22

According to some estimates, the IAA has blocked or shut down at least 1,000 websites, including human rights websites, blogs, online forums, and individual pages from social media networks.23 A crowdsourced list of 367 blocked websites reported in early 2015 that 39 percent of blocked sites were related to politics, while 23 percent were related to the use of various internet tools, such as anonymizers and web proxies.24 Many of the websites were targeted for blocking after the 2011 protests, which were called for and heavily covered by online channels, resulting in a significant rise of blocking and filtering measures by the Bahraini authorities.25 Meanwhile, the websites of the Arab Network for Human Rights Information (ANHRI) and the Bahrain Center for Human Rights (BCHR) have been blocked since 2006. In November 2013, following a campaign by the BCHR to expose officials and royal family members involved in violations, an alternative link to the center’s website was blocked as well.26

Although there are a number of news websites providing a plurality of viewpoints that are distinct from the Bahraini state media narrative, most of these are blocked by the government and require circumvention tools to access. Bahrain Online, a prominent online forum, has been blocked since its

---

launch in 1998. The Arabic web portal and blog-hosting service Al-Bawaba has also been blocked since 2006. Online newspapers have been banned from using audio and video reports on their websites since 2010, apart from the state-owned Bna.bh, which broadcasts video from state television. The popular Bahraini online news website Bahrain Mirror has been blocked since its launch in 2011. According to the website’s administration, the government has blocked more than six alternate addresses since then.

In August 2013, the communications minister ordered ISPs to block 70 websites that were supposedly “affiliated with internationally recognized organizations that fund and promote terrorism.” The minister also ordered telecom companies to take measures against text messages sent from abroad that promote violence. While some sites affiliated with Hezbollah, al-Qaeda, and other groups were blocked, others remained accessible, giving a sense that the fight against terrorism is being used as an excuse to censor online content from dissidents.

YouTube, Facebook, Twitter, and international blog-hosting services are freely available. However, other applications are permanently blocked, and specific content on social networks can be inaccessible. For example, since the 2011 protests, most live-broadcasting websites that were popular among protesters have been blocked. PalTalk, a chatting service that was used to conduct political seminars for wide online audiences, has been blocked since June 2011. In November 2013, Matam.tv, a website that broadcasts live religious events and sermons from Shi’a religious centers across Bahrain, was reported blocked prior to religious commemorations surrounding the predominantly Shi’a anniversary of Ashura.

Websites are filtered based on keyword density, the manual entry of URLs, and certain website categories. An updated list of blocked websites is regularly sent to ISPs, which are instructed to “prohibit any means that allow access to sites blocked by the ministry.” Through IAA notification, the TRA can revoke the license of any operator that does not cooperate with IAA blocking orders. Batelco, Bahrain’s main ISP, filters the web using McAfee SmartFilter software and Blue Coat technology.

---

32 The websites of Al-Qaeda and Al Nusrah Front remain accessible as of 10 Jan 2014, see, Bahrain Freedom Index (blog), http://bit.ly/1DhNJhF.
Bahrain

March 2011, plans were announced to switch to technology from Palo Alto Networks that can block certain elements and activities within websites, such as video or photo uploading, and make it more difficult for users to circumvent censorship. In August 2014, the company announced a partnership with the largest ISP in the country, Batelco, though it is unclear whether its blocking tools have been implemented.

The decision-making process and government policies behind the blocking of websites are not transparent. The list of all blocked websites is not available to the public. In addition, webmasters do not receive notifications or explanations when their websites are banned. When trying to access a blocked site, users are presented with the message, “This web site has been blocked for violating regulations and laws of Kingdom of Bahrain,” with no particular laws specified. Although the law does technically allow affected individuals to appeal a block within 15 days, no such case has yet been adjudicated.

Content Removal

Authorities also use extralegal measures to forcibly remove online content. Through the use of arrests, detentions, and torture, security forces coerced many online forum moderators into permanently shutting down their sites following the 2011 crackdown. This resulted in the loss of a large amount of information on Bahrain's history that had been documented by online users and in local forums and websites. Website administrators face the same libel laws that apply to print journalists and are held jointly responsible for all content posted on their sites or chat rooms.

In June 2014, around 97,000 tweets were apparently erased from the well-known account of the satirical Twitter user “@Takrooz” after he was arrested. The account was critical of both the government and the opposition, with over 17,000 followers. Only one tweet remains posted on the account, stating, “They tortured me in prison,” though the actual ownership of the account remains a mystery since the alleged account holder remains in prison and denies ownership. Responsibility for deleting the tweets was also unclear. In the same month, another famous Twitter account, “@mnarfezhum,” was forcefully suspended after reports that its operator, a member of the royal family, was under prosecution. With over 97,000 followers, @mnarfezhum mainly attacked and incited arrest and punishment against prodemocracy protesters, although the user later sent threats to the interior ministry for trying to hack the account (for more, see “Prosecutions and Detentions”). In September 2014, Ghada Jamsheer, an active Twitter user and government critic whose blog had been blocked for several years, was forced to close her account after repeated arrests and several weeks spend in detention.

---

42 Moderator of the AlDair Forum talks about his detention, saying he was forced to show the interrogation officer how to close the website: “Ahmed al-Dairi Moderator of AlDair Forums in the first episode of his testimony: thus eased voice of Zakaria AlSheeri forever,” [in Arabic] Bahrain Mirror, January 4, 2012, http://bahrainmirror.com/article.php?id=2678&cid=117
43 Snapshot of the account page before tweets were erased see, Bahrain Freedom Index http://bit.ly/1UeMgpwp.
Bahrain

In July 2014, a YouTube video went viral in which an exiled Bahraini activist, Moosa Abdul-Ali, accused the Bahraini chief of public security and an Interior Ministry spokesperson of human rights abuses while speaking with them in Geneva. After gaining 83,000 views, the video was taken down by YouTube on copyrights grounds even though it did not apparently include any copyrighted materials. The video was reinstated within a few days after resolving the matter with Google, YouTube’s parent company. Meanwhile, Twitter received no requests from Bahraini authorities to restrict content during the coverage period, according to the company’s latest transparency report.

News outlets also faced pressure to remove content. In August 2014, al-Wasat newspaper removed an article from its website as a result of a defamation complaint filed by members of the “Baluch” family in Bahrain, which has old connections to the Baluchistan region of modern day Pakistan. The article was based on British documents from the 1920s that discussed the employment of foreign forces of Baluchistani origin—to which the family holds connections—in the Bahraini police force, calling those forces “mercenaries.”

Media, Diversity, and Content Manipulation

The authorities are known to manipulate online content in order to fabricate greater public support. According to the independent watchdog group, Bahrain Watch, the government has hired 18 public relations (PR) firms for promotional campaigns since February 2011, representing at least USD 32 million in contracts. At least one PR agency was contracted to provide “web optimization and blogging” services, while others were hired for online reputation management. In October 2014, one of these PR companies tried to force The Huffington Post not to write on the United Kingdom’s investigation of torture allegations against the Bahraini king’s son. Meanwhile, hoax journalists spread propaganda on Twitter and progovernment blogs such as Bahrain Views and Bahrain Independent.

Similarly, an “army of trolls” has been active on Twitter since February 2011, when hundreds of accounts suddenly emerged to collectively harass and intimidate online activists, commentators, and journalists who voiced support for protests and human rights. The government trolls have been...

58 J. David Goodman, “‘Twitter Trolls’ Haunt Discussions of Bahrain Online,” The Lede (blog), The New York Times, October 11,
moderately effective in silencing or reducing the activity of opposition voices both inside Bahrain and abroad. The trolls have also played a vital role in spreading information that is controversial, offensive, or false, in order to distort the image of protesters, spread hate and conflict, or discredit information posted on social networks. These troll accounts usually have few followers (or sometimes none at all) and tend to appear and disappear in coordination with one another.

In August 2013, Bahrain Watch revealed evidence of connections between the Bahraini government and "extremist" accounts on Twitter and Facebook that advocated violence against both the government and protesters. It was also revealed that the government impersonates opposition figures on social media in order to send malicious links, such as IP trackers, to anonymous government critics that can be used to identify and prosecute them. In January 2014, the prime minister and the minister of telecommunications held several public meetings with progovernment users to encourage them to "defend Bahrain's ruling system."

The state also issues official statements warning against the discussion of certain subjects. Most recently in March 26 2015, the Interior Ministry issued a statement warning it would take steps against anyone expressing opinions “against the approach that Bahrain has taken” in supporting and joining the Saudi-led coalition conducting airstrikes in Yemen (see “Prosecutions and Detentions”).

Despite these numerous attempts to manipulate the online information landscape, government restrictions on online advertising have not forced the closure of any opposition websites. While it is difficult for blocked websites to secure advertising, popular sites such as Bahrain Mirror (390,000 views monthly) have not faced significant financial pressures. This is due to the fact that most Bahraini opposition websites are run with limited and sometimes personal resources. Furthermore, the websites continue to receive large amounts of traffic from users within Bahrain through the use of proxy services, dynamic IP addresses, and virtual private network (VPN) applications. However, the government does regularly block access to circumvention tools, including techniques such as using Google Page Translate, Google cached pages, and online mobile emulators. Adaptive and internet savvy Bahrainis tend to find ways around these restrictions.

The internet is also the main source of information and news for many Bahrainis, particularly those active on Twitter and Facebook. The number of Bahraini users on Facebook increased to around 540,000 as of May 2014, representing a penetration rate of nearly 39 percent. The #bahrain hashtag
remains one the most popular topics on Twitter across the Arab region, with around 710,000 tweets on the English hashtag and 1,000,000 tweets on the Arabic hashtag of Bahrain in March 2014 alone.68

The government crackdown in March 2011 led many regular internet users to exercise a higher degree of self-censorship, particularly after investigations of users’ online activities were launched at work places and universities.69 Twitter and online forum users, and even those who leave comments on online editions of newspapers, use pseudonyms due to fear of being targeted by the authorities.70 Many have modified their privacy settings on social media or “protected” their Twitter pages. Some temporarily stopped tweeting after receiving threats to their personal safety.71 As a result, the number of active Bahraini Twitter users has dropped in recent years,72 from 72,468 reported in June 2012,73 to 62,200 in March 2014.74

Digital Activism

Given restrictions on press freedom, the lack of international media coverage, and the inability of many prominent journalists to enter the country,75 activists rely on digital tools to bring attention to protests and human rights violations.76 This past year saw the rise of a new trend of leaked photos and videos uploaded to the internet by prisoners exposing harsh conditions. In February 2015, a video was uploaded on YouTube with the testimony of Abbas al-Sameea,77 a prisoner who had received the death penalty in an unfair and politicized trial. That same month, a group of prisoners staged a protest and launched an online campaign on overcrowded conditions inside the central prison.78 In March, authorities responded to the protests with mass punishment and attacked the prisoners with tear gas and shotguns in their closed cells.79 The photos of the attack were posted directly to the internet by prisoners, catching the attention of local80 and international human rights NGOs,81 which have since issued several statements for the protection of prisoners’ rights. In response, the prison

68 “Citizen Engagement and Public Services in the Arab World: The Potential of Social Media,” in Arab Social Media Report, Figure 40.
71 “Bahrain doctor @BAHRAINDOCTOR threatened with arrest because of her tweets,” Bahrain Freedom Index (blog), accessed July 31, 2015, http://bit.ly/1QDPIkU.
72 As officially defined by Twitter, an “active user” is someone who logs in (but does not necessarily tweet) once a month.
74 “Citizen Engagement and Public Services in the Arab World: The Potential of Social Media,” in Arab Social Media Report, Figure 32.
75 “Access Denied,” a project of the independent research and advocacy organization Bahrain Watch, chronicles the many journalists, researchers, academics, and NGO workers that were expelled from or denied access to Bahrain from the 2011 uprising until now. See, http://bahrainwatch.org/access/.
77 “Video of Abbas al-Samiee’s message to the people on his imprisonment and death sentence,” [in Arabic], YouTube video, 8:55, posted by BahrainAlyoum, February 26, 2015, https://www.youtube.com/watch?v=HWpSnIkK3368.
authority cut off all authorized prisoners’ communications with the outside world to minimize leakage of information of the attack’s aftermath, though tweets on injuries and prison conditions continue to emerge.82 In June, the Office of the UN High Commissioner for Human Rights (OHCHR) issued a statement raising concerns on their conditions.83

The resilient social protest movement titled the “Coalition of February 14 Youth” continues to use social networks,84 both to organize protests and bring international mainstream media attention to local causes.85 In December 2014, the BBC reported the mysterious disappearance of a Bahraini citizen at the hands of security forces after a related hashtag gained popularity on Twitter.86 YouTube videos are also uploaded to document police attacks on civilians and torture testimonies,87 though some are promptly blocked.88 Relatives or friends of detainees regularly use Twitter to campaign for their release and provide updates about prison conditions.89 Overall, by uploading videos and sharing images on social media, protesters have maintained the spotlight on their struggle.

Violations of User Rights

Violations of user rights in Bahrain were rampant, with at least 27 users arrested, detained, or prosecuted over the coverage period. Collectively, 27 months of prison sentences were passed down to 11 users, while others remain on trial or in arbitrarily detention. Bahraini law does not contain adequate protections for free speech, given provisions that ban criticism of the royal family, the spreading of false news during war, or insulting the foreign politicians. A computer crimes law passed in December 2014 criminalizes the access or possession of online electronic pornography as well as the use of encryption for “criminal purposes.” The broad wording of the latter provision has worried activists who depend on encryption tools to document human rights abuses and speak freely on political matters, activities that are routinely considered criminal acts in the country.

Legal Environment

Bahrain’s legal environment presents many obstacles to internet freedom in its current form. According to Article 23 of the Bahraini constitution, freedom of expression is guaranteed, “provided that the fundamental beliefs of Islamic doctrine are not infringed, the unity of the people is not prejudiced, and discord or sectarianism is not aroused.”90 Article 26 states that all written, telephonic, and electronic communications “shall not be censored or their confidentiality be breached except in exigencies specified by law and in accordance with procedures and under guarantees prescribed by the
Bahrain

law."91 The Press and Publications Law of 2002 promises free access to information “without prejudice to the requirements of national security and defending the homeland.” Bahraini journalists have argued that these qualifying statements and loosely-worded clauses allow for arbitrary interpretation and, in practice, the negation of the many rights they seek to uphold.92 In addition, there is no law that defines clear penalties for violating the privacy of internet users, a concern for many bloggers who believe this allows for abuse.93

Numerous regulations related to the internet proposed since 2011 signal a negative trend in the country’s legal environment. Official announcements in 2012 indicated preparations to introduce tough new laws to combat the “misuse” of social media,94 after information spread online about the identities of security officers involved in human rights violations.95 In September 2013, the cabinet green-lighted new legislation that would criminalize anyone who establishes a website, publishes information online, or uses any information technology tool to assist or aid communications with terror cells or to promote the disruption of public order or morale.96 The law has not been passed as of mid-2015.97 In August 2014, the prime minister renewed calls to take immediate measures to control the usage of social media and to hold the “abusers” of these networks accountable.98 This was followed by similar directives from the Bahraini king to fight the “wrongful use” of social media by legal means.99

Online censorship and criminal penalties for online speech are currently enforced under the 2002 Press and Publications Law,100 which does not specifically mention online activities but was extended to mobile telephones in 2010.101 The law allows for prison sentences from six months to five years for repeat offenders, for publishing material that criticizes Islam, its followers, or the king, as well as content that instigates violent crimes or the overthrow of the government.102 In addition, the 2002 Telecommunications Law contains penalties for several online activities, such as the transmission of messages that are offensive to public policy or morals.103 However, sentences can be longer if users are tried under the penal code or terrorism laws. For instance, under the penal code, any user who “deliberately disseminates a false statement” that may be damaging to national security or public

91 Constitution of the Kingdom of Bahrain, art. 26.
100 For cases where the authorities have used the 2002 press law to censor online websites, see BCHR, “Website accused of violating press code, BCHR concerned that move is aimed at silencing critical voices,” October 1, 2008, http://www.bahrainrights.org/en/node/2446.
103 The Telecommunications Law Of The Kingdom Of Bahrain, Legislative Decree 48.
order can be imprisoned for up to two years. The government has used these vague clauses to question and prosecute several bloggers and online commentators.

Prosecutions and Detentions for Online Activities

Between June 2014 and May 2015, at least 27 online users were arrested, detained or prosecuted for their ICT activities. While the majority of users are still on trial as of mid-2015, 29 months of prison sentences were collectively passed down on 11 Bahraini users in cases directly related to online posts between June 2014 and May 2015; meanwhile, 12 users remain in jail. As photos and videos of police brutality emerged online, more measures were taken against citizens who were targeted for holding cameras, including smartphones, in protest areas. Meanwhile, bloggers, moderators, and online activists were systematically detained and prosecuted by the authorities for expressing views the government regards as controversial. Most prosecutions during the coverage period involved Twitter and the charge of “insulting the king,” which carries criminal penalties that, in February 2014, were increased to a maximum of seven years imprisonment.

Nabeel Rajab, one of Bahrain’s most prominent human rights defenders and most followed Bahraini Twitter user (@NabeelRajab), has been in-and-out of prison since 2012 on various cases linked to his tweets. Rajab is the president of the Bahrain Center for Human Rights, a nongovernmental organization that remains active despite a 2004 government order to close it. Nearly four months after completing a two-year prison sentence for “calling for illegal gatherings over social networks,” Rajab was arrested on October 1, 2014 and charged with insulting public institutions under article 216 of the penal code for a tweet in which he questioned whether Bahraini security institutions are “ideological incubators” for the terrorist group the Islamic State in Iraq and Syria (ISIS). He was released on November 2, 2014 under a travel ban and later handed a suspended six month prison sentence upon payment of a BHD 200 (USD 533) fine on January 20, 2015. He was subsequently targeted for arrest again on April 2 on charges of “spreading false news in a time of war” and “insulting a statutory body” for tweets about the Saudi-led coalition airstrikes in Yemen and the alleged...
torture of detainees at Jaw prison.  

Numerous other individuals were arrested and/or prosecuted for criticizing the authorities online during the coverage period:

- On May 27, 2014, the public prosecutor announced an investigation into two individuals suspected of involvement with the Twitter account @mnarfezhom, a known progovernment account with 97,000 followers, on charges of “instigating hatred against the regime, threatening public peace and security, insulting state institutions, disseminating confidential security reports, and defamation of several persons.” Owned by a member of the royal family, Mohamed Salman Saqer al-Khalifa, the account began by reporting on protestors and defaming opposition figures, but eventually evolved, attacking other progovernment groups with differing opinions. It consistently published important news before any official source. Although many have lodged complaints with the public prosecution against the account, no action had been taken during the past three years. Things appeared to have changed when @mnarfezhom posted that the Interior Ministry had tried to hack the account, and threatened to publish a list of Twitter accounts operated by the ministry and the national security apparatus, as well as the names of ministry staff who participated in the 2011 online campaign against the protests. The tweets led the prosecutor to crackdown on the account, arresting two individuals from an office where they were allegedly preparing videos to post online. The users were later released the same day but were rearrested on June 5, 2014. On June 11, AlAyam newspaper published an apology from the supposed owner of the @mnarfezhom Twitter account, which was directed to a victim of one of his defamatory tweets. One week later, the two detained users were released on bail of BHD 200 (USD 533) and issued a travel ban. As of mid-2015, two defamation cases are pending against them in court.

- On August 31, 2014, progovernment activist Yacoub al-Slaise was briefly detained over a tweet in which he mentioned that votes by military personnel in the upcoming parliamentary elections are likely to be controlled by the state. He was charged with “defaming the army” and released the next day. On February 10, 2015 a court ordered him to pay a fine of BHD 200 (USD 533).  

---

123 BCHR, “Bahrain After Directives From The King And The Prime Minister: The Campaign On Social Media Activists Escalates.”
On December 25, 2014, former MP Khalid Alaal was summoned for interrogation over tweets critical of the interior ministry that he posted while he was still an active MP in April 2014. He was charged with “insulting the Ministry of Interior” and, on May 26, 2015, sentenced to one year in prison. However, as of mid-2015, he had not been imprisoned.

In the early hours of February 10, 2015, the authorities raided the home of social media activist Jaleela al-Sayed Ameen, confiscated her electronic devices, and detained her on charges of misusing social media, inciting hatred against the regime, and insulting the king. She was reportedly subjected to ill-treatment while held at the criminal investigation department and was later taken to the prison hospital. She was denied contact with her family or lawyer for several days after her arrest and denied visits from her family until the beginning of March. As of mid-2015, she remained in detention while her trial was ongoing.

On March 26, 2015, Fadhel Abbas, General Secretary of the Democratic Unity Gathering Society was arrested shortly after the society released a statement on Twitter condemning the war against Yemen. He was sentenced to five years in prison in June 2015.

In the period leading up to the November 2014 parliamentary elections, several users were arrested for their criticism of the elections, including a former member of parliament (MP):

- On November 15, 2014 Mukhtar al-Saffar was arrested after a YouTube video of him calling for a boycott of the elections and harshly criticizing participants went viral. He was released on bail of BHD 50 (USD 134) on November 27, 2014, and his trial was ongoing as of mid-2015.
- Well-known satirical actor, Mansoor Senqaimah, was referred to the public prosecution in November 2014 and interrogated for defamation over a YouTube video in which he criticized a former MP.
- On October 9, 2014, former opposition MP Sayed Jameel Kadhem was interrogated over a tweet in which he mentioned that up to BHD 100,000 of “political money” was paid to people affiliated with the opposition to run for seats in the widely boycotted November 2014 parliamentary elections. On January 13, 2015, a court sentenced him to six months in prison and a fine of BHD 500 (USD 1,326) on charges of “disturbing elections” and he was...
Bahrain

arrested the next day. A court of appeal upheld the sentence against him on February 15, 2015. Users were further targeted for satirical content. On June 15, 2014, Bahrain arrested Hussain Mahdi upon arrival to Bahrain airport from Thailand and accused him of operating the satirical Twitter account “@Takroz” known for its harsh criticism of both the opposition and government. Charged with “inciting hatred against the regime” and “using expressions that incite sectarianism,” Mahdi has been in detention and awaiting trial since his June 2014 arrest. He has denied connections to the account, which had all 97,000 of its tweets erased following Mahdi’s arrest, with the exception of one that was posted after his arrest, stating: “They tortured me in prison.” Before the arrest, @Takroz was constantly targeted by the Bahrain Cyber Crime Unit with malicious links sent in a bid to identify the user’s IP address.

Social media users were also heavily targeted for alleged blasphemy. Online hate speech against religious figures dignified by Shia Muslims often takes place with impunity, while posts seen to insult the sensitivities of the country’s minority Sunni population, which includes that of the royal family, are heavily censored.

On August 27, 2014, activist Nader Abdulemam was arrested after three people accused him of “denigrating the prophet’s companion Khalid Bin al-Waleed” in a tweet he posted telling a historical story in which Khalid killed another companion and raped his wife. He was sentenced to six months in prison on October 22, 2014, which was later reduced to four months on January 15, 2015, when he was released for serving more time than his sentence. Repression against Nader continued when he received news on March 5, 2015 that he was dismissed from his job as a teacher at the ministry of education, where he had worked for the past 14 years. Authorities also arrested two Instagram users in September 2014 on charges of “denigrating the prophet’s companions.”

The death of King Abdullah of Saudi Arabia in January 2015 led to a wave of controversial social media posts in Bahrain, given the role of Saudi Arabia in sending troops to Bahrain to crack down
on peaceful protestors in February 2011. Eleven users, including two teenage girls, were arrested for critical posts about the late Saudi king.\textsuperscript{147} The girls were released after two days. Nine young men were referred to the court on charges of “misusing social media” based on article 215 of the penal code, which provides for “a jail term of up to two years or a fine of up to BD200” for “anyone who offends in public a foreign country or its president or representative.” In March, four of the nine were each sentenced to three months in prison, while one was acquitted; the remaining four were still on trial as of mid-2015.\textsuperscript{148} Additionally, the names and pictures of defendants were posted on the website of the interior ministry and on state media.\textsuperscript{149}

Several Bahraini photographers faced reprisals, often through trumped up charges, for documenting protests and posting their images online:

- Award-winning photographer Ahmed Humaidan, who was arrested in 2012, was sentenced to 10 years in prison for allegedly participating in an attack on a police station in the district of Sitra,\textsuperscript{150} though it is believed he was targeted for photographing protests.\textsuperscript{151}

- Photographer Hussain Hubail, detained since July 31, 2013, was sentenced on April 28, 2014 to five years in prison on charges of “inciting hatred against the regime through social media, and calling for illegal protests” after a trial that lasted around five months.\textsuperscript{152} His appeal was rejected on September 21, 2014.\textsuperscript{153}

- Photographer Ahmed Al-Fardan, who uses photo-sharing platforms like Instagram and Demotix, was arrested in the early hours of December 26, 2013 without a warrant and disappeared for over a week. He was subject to torture that resulted in two broken ribs,\textsuperscript{154} and interrogated without a lawyer present on charge of “intending to participate in illegal gatherings.”\textsuperscript{155} He was released on January 9, 2014 following pressure from international media watchdogs.\textsuperscript{156} However, on February 18, 2015, he was sentenced to three months in prison and a bail of BHD 100 Bahraini dinars to suspend the sentence during appeal.

In addition to individuals, civil society actors were subject to prosecution for their online posts. On February 16, 2015, the ministry of interior announced it is preparing to prosecute Alwefaq Islamic Society, the largest political group in Bahrain, over posts on its website and Twitter account.

\begin{enumerate}
\item 148 “Three months imprisonment for the accused of abuse to an Arab country,” [in Arabic] AlWasat, March 24, 2015, http://bit.ly/1ojY1KR; Manama Voice, Twitter Post, April 28, 2015, 8:20 PM, “Three sentenced to three months imprisonment each and the fourth is acquitted from charges of abuse to an Arab country,” [post originally in Arabic] https://twitter.com/manamavoice1/status/59325344230146048.
\end{enumerate}
Bahrain

Legedly inciting hatred against the regime and spreading of false information.\textsuperscript{157} The society actively posts information and photos of the ongoing human rights violations including arrests, torture, attacks on protests, and the excessive use of tear gas in residential areas.\textsuperscript{158}

Meanwhile, the two harshest sentences ever passed on Bahraini internet users—life in prison and 15 years—remained in place against bloggers, Abduljalil al-Singace and Ali Abdulemam, who were separately charged with possessing links to a terrorist organization aiming to overthrow the government,\textsuperscript{159} disseminating false news, and inciting protests against the government. Al-Singace, a prominent human rights defender and blogger, has been serving a life sentence since March 2011,\textsuperscript{160} and his blog has been blocked since 2009.\textsuperscript{161} Abdulemam, the owner of Bahrain’s popular blocked online forum, Bahrain Online, received a 15-year sentence in absentia in 2013 and is currently a political refugee in the UK. He had previously spent two years in hiding in Bahrain.\textsuperscript{162} Both reported experiencing torture at the hands of the authorities.\textsuperscript{163}

**Surveillance, Privacy, and Anonymity**

A computer crimes law that had been under review since 2005 was finally approved by the House of Representatives and ratified by the government in December 2014. The new law (60/2014) criminalizes the illegal access of information systems, illegal eavesdropping over transmission, or the access and possession of pornographic electronic materials.\textsuperscript{164} It also criminalizes the encryption of data with criminal intentions at a time when freedom of expression is often considered a criminal act in Bahrain.

In August 2014, a new report provided evidence that the Bahraini government obtained licenses of the malicious FinFisher spy software to spy on at least 30 computers simultaneously. The list of identified victims included the country’s most prominent lawyers, activists and politicians.\textsuperscript{165} Evidence has also been documented about the use of spy gear maintained by Nokia Siemens Networks and its divested unit Trovicor to monitor and record phone calls and text messages.\textsuperscript{166} Similarly, researchers discovered malicious software concealed in seemingly innocent emails sent to Bahraini activists in April and May 2012. The surveillance software, FinFisher, is developed by the Munich-based Gamma International and distributed by its U.K. affiliate, Gamma Group. One feature of the software, FinSpy, enables law enforcement to remotely take control of a computer to take screen shots, intercept VoIP.

\textsuperscript{157} Police Media Center “Documenting abuses of the Alwefaq Society that constitute criminal offenses punishable by law, as a prelude to referring the case to the prosecutors and to raise a lawsuit against the Society.” [in Arabic] February 16, 2015, \url{http://bit.ly/17j1VHu}
\textsuperscript{158} Alwefaq Society, Twitter Account, \url{https://twitter.com/ALWEFAQ}
\textsuperscript{160} Reporters Without Borders, “Detained blogger Abduljalil Al-Singace on hunger strike.”
\textsuperscript{163} “People & Power – Bahrain: Fighting for change,” YouTube video, 24:30, posted by Al Jazeera English, March 9, 2011, \url{http://bit.ly/1Flun6y}
\textsuperscript{164} General Directorate of Anti-Corruption & Economic & Electronic Security, Law No. (60) for the year 2014 on information technology crimes, [in Arabic] accessed July 31, 2015, \url{http://bit.ly/1QMe8FR}
\textsuperscript{165} Bahrain Watch, “Bahrain Government Hacked Lawyers and Activists with UK Spyware,” August 7, 2014, \url{http://bit.ly/1q0tMP9}
\textsuperscript{166} Vernon Silver and Ben Elgin, “Torture in Bahrain Becomes Routine With Help From Nokia Siemens,” Bloomberg Business, August 22, 2011, \url{http://bloom.bg/1MkkAoQ}
calls, and transmit a record of every keystroke. The company denied selling to the Bahraini government, saying that the version of FinSpy deployed on activists was “old” and for demonstration purposes only. However, research published in 2013 shows that a newer version of the FinSpy software is also in use in Bahrain, suggesting the government is receiving paid updates from the company.

Given that the authorities have been quick to identify social media users who operate under a pseudonym, many users are concerned about restrictions on the ability to use ICT tools anonymously. The TRA requires users to obtain licenses to use Wi-Fi and WiMax connections, and the government prohibits the sale or use of unregistered prepaid mobile phones. Cybercafes are also subject to increasing surveillance. Oversight of their operations is coordinated by a commission consisting of members from four ministries, who work to ensure strict compliance with rules that prohibit access for minors and require that all computer terminals are fully visible to observers. In May 2014, the government announced that it is considering new restrictions on cybercafes, including the enforcement of surveillance cameras as well as storage of user’s personal identification and activity.

Since March 2009, the TRA has mandated that all telecommunications companies keep a record of customers’ phone calls, emails, and website visits for up to three years. The companies are also obliged to provide the security services with access to subscriber data upon request. Following implementation of the National Safety Status emergency law in March 2011, security personnel began searching mobile phones at checkpoints, behavior that was documented on YouTube. According to Twitter’s Transparency Report, the Bahraini government requested data about one user account in the first six months of 2014, but no data was produced. Similarly, the Facebook’s Transparency Report shows that the Bahraini government requested data about one user account in the first six months of 2014, but no data was produced.

A new Cyber Safety Directorate at the Ministry of State for Telecommunications Affairs was launched in November 2013 to monitor websites and social media networks, ostensibly to “ensure they are not used to instigate violence or terrorism and disseminate lies and fallacies that pose a threat to the kingdom’s security and stability.” The IAA had earlier created a unit to monitor social media and foreign news websites to “respond to false information that some channels broadcast” in 2011, when it was run by the telecommunications ministry.

Although most online users use nicknames, authorities use malicious spy links to identify users

---


through their IP address. Links are often sent from Twitter and Facebook accounts impersonating well-known opposition figures, friends, or even accounts of arrested users. In addition, police often entrap users using fake names. On September 3, 2014, 15 users of the Zello Walkie Talkie mobile app were arrested after the police infiltrated three Zello groups and posted an invitation to a fake meeting where they were detained.

Intimidation and Violence

 Typically, arrests of Bahraini users involve extralegal methods of intimidation, such as physical violence and torture. Lawyer Mohamed al-Tajer said that Hussain Mahdi, who was arrested for operating the Twitter account (@Takrooz) was beaten, tortured, and threatened with sexual assault and electricity shocks to force his confessions.

The government has also used extralegal methods to punish users for their online posts. On January 31, 2015 the ministry of interior revoked the citizenship of renowned blogger Ali Abdulemam, as well as Ali al-Dairi, the founder of the popular news site Bahrain Mirror. Both are currently living abroad and continuing their digital activism for democracy in exile.

Since 2011, numerous students and employees have received disciplinary action for comments they have communicated via private text messages and social media. On September 8, 2014, the ministry of education suspended an employee from work and cut her salary for 10 days over a WhatsApp message that allegedly “insulted the state leadership figures.” In October 2014, the ministry of education interrogated its own security guards over political text messages shared over mobile phone chatting apps. The guards were shown snapshots of their chat conversations as evidence and were asked to delete the “illegal” political chat groups from their phones, while the group admins were forced to stand under the sun for several days. Some were moved to other work sites that are far from their residence as a punishment. Also, in September 2014, an employee of the ministry of culture was interrogated over an Instagram photo of her standing next to renowned human rights defender Nabeel Rajab.

---

Bahrain

Technical Attacks

Cyberattacks against opposition and progovernment pages, as well as other websites, are common in Bahrain. Accounts operated by the opposition are frequently subjected to mass reporting campaigns to have them closed by Twitter.188

According to official statistics, there were 1,115 cyberattacks during first quarter of 2014 on government websites in attempt to take over the sites or manipulate content.189 Additionally, at least 40 sources of malicious emails were identified inside Bahrain by MacAfee.190 Government-associated websites are frequently targeted with distributed denial of service (DDoS) attacks.

188 Bahrain Detainees, Twitter post, May 12, 2015, 8:23 AM, A tweet mentioning one opposition accounts that has been suspended due to reports, accessed July 31, 2015 https://twitter.com/BH14Detainees/status/598146464934547456.
Key Developments: June 2014 – May 2015

- Four bloggers were murdered in 2015, allegedly by religious extremists. Abhijit Roy, Washiqr Rahman, Ananta Bijoy Das, and Niladri Chattopadhyay Niloy were fatally attacked in separate incidents in February, March, May, and August of 2015 respectively (see Intimidation and Violence).

- In September 2014, a local court sentenced a mobile phone user to seven years in prison under the ICT Act (see Prosecutions and Detentions for Online Activities).

- The BTRC briefly blocked social messaging applications for four days in January 2015 in relation to political violence (see Restrictions on Connectivity).

- Campaigners across the political spectrum embraced digital tools in advance of local elections in two major cities (see Digital Activism).
Bangladesh

Introduction

The year 2015 saw the highest number of fatal attacks against online activists in Bangladesh on record. Abhijit Roy, Washiqur Rahman, Ananta Bijoy Das, and Niladri Chattopadhyay Niloy were fatally attacked, each in separate incidents in 2015, in reprisal for views they had expressed online. Attacks on secular bloggers started in 2013, when Asif Mohiuddin was first attacked by extremists, and blogger Ahmed Rajib Haider was killed outside his home. Censorship did not increase in the past year, but the attacks, combined with the threat of arrest under the ICT Act, created a climate of intimidation that fostered self-censorship and mistrust.

The government of the Bangladesh Awami League party under Prime Minister Sheikh Hasina officially encourages open internet access and communication as core tools for development. Private commercial stakeholders have also helped in the proliferation of internet usage. Bangladesh further benefits from a vibrant—if often partisan—traditional media industry, though journalists face threats and legal constraints.

Checks on bloggers and online activity are arguably harsher due to the 2006 Information and Communication Technology (ICT) Act. The act was used for the first time in April 2013 to arrest four bloggers who had been vocal on different social issues and mostly wrote against religious extremism. By August 2013, an amendment was passed increasing the penalty to a minimum of 7 years, up to 14 years in prison. Police no longer need a warrant to make arrests under the amended act, and the number of prosecutions is increasing. In September 2014, a local court sentenced a 25 year old to seven years in prison under the ICT Act for recording songs which parodied the prime minister and the father of the nation and sharing them on his phone. At least two other arrests were made for comments involving the prime minister.

Obstacles to Access

The number of internet users in Bangladesh is steadily on the rise. Approximately 96 percent of users access the internet via mobile phone providers, which recently began offering faster 3G service. The government has decreased the price of bandwidth significantly over the last decade. However, users complain about the high cost of private internet service.

Availability and Ease of Access

The International Telecommunication Union reported internet penetration in Bangladesh at 9.6 percent in 2014, up from 6.6 in 2013. Government estimates were closer to 30 percent. Mobile penetration rose from 74 in 2013 to 76 in 2014, according to the Bangladesh Telecommunication Regulatory Commission. While ICT usage is increasing fast, Bangladesh is lagging behind globally. The World Economic Forum’s 2013 global IT report ranked Bangladesh 114 out of 144 countries worldwide, with infrastructure and regulatory environment scoring poorly, though overall communication

service was comparatively affordable, a factor that is driving growth.\textsuperscript{5} The government has decreased the price of bandwidth significantly over the last decade.\textsuperscript{6} However, users complain about the high cost of private internet service. The ability to access localized information and create content in Bengali has contributed to the popularity of local blog hosting services.\textsuperscript{7}

Although no statistics are available, the higher concentration of economic activities and critical infrastructure in urban areas indicates there are likely to be more internet users in cities. The government’s 2009 “Digital Bangladesh by 2021” program seeks to integrate internet access with development efforts in national priority areas, such as education, healthcare, and agriculture.\textsuperscript{8} By 2011, the government had established 4,501 centers around Bangladesh providing low-cost internet access and related e-services in poorer communities.\textsuperscript{9}

**Restrictions on Connectivity**

The government occasionally restricts the use of mobile telephones during the time of local and national elections. On January 2015, the government briefly blocked mobile voice and messaging applications to curb violence (see Blocking and Filtering).

Bangladesh’s physical internet infrastructure was historically vulnerable, relying on the undersea cable SEA-ME-WE-4, which connects Southeast Asia, the Middle East, and Western Europe, for its backbone.\textsuperscript{10} Since late 2012, however, Bangladesh is also connected via an international terrestrial cable managed by private companies, reducing the risk of being completely cut off.\textsuperscript{11}

**ICT Market**

Approximately 96 percent of users access the internet via mobile phone providers, which only recently began offering faster 3G service. The remainder subscribe to fixed lines, either through a traditional internet service provider (ISP), the fixed telephone network (around three percent), or via one of the three wireless WiMax operators (one percent).\textsuperscript{12} In 2014, 61 ISPs were operating nationwide as members of the official industry body, the ISP Association of Bangladesh.\textsuperscript{13}

Mobile connections are provided by six operators.\textsuperscript{14} Grameen Phone, owned by Telenor, is the mar-
ket leader with 42 percent of the total customer base, followed by Orascom’s Banglalink with 26 percent, and Robi, under the Axiata company, with 21 percent. The remaining three, Airtel, Citycell, and the state-owned Teletalk, had a total customer base of 11 percent at the end of 2014. As of 2015, all except Citycell offered 3G services.15

Regulatory Bodies

The Bangladesh Telecommunication Regulatory Commission (BTRC), established under the Bangladesh Telecommunications Act of 2001, is the official regulatory body overseeing telecommunication and related ICT issues in Bangladesh. However, the current administration amended the act in 2010, passing telecommunications regulation to the Ministry of Post and Telecommunications and making the BTRC an auxiliary organization.16 This move created administrative delays in a number of basic processes like the announcement of new tariffs or license renewals.17 Recently, the Ministry of ICT merged with the Ministry of Post and Telecommunications, with the goal of streamlining many ongoing projects and related industries.18 In addition, the prime minister’s office has an Access to Information (A2I) program supported by the United Nations Development Program, which has considerable influence over top-level ICT-related decision making.19

Limits on Content

The BTRC briefly blocked a handful of communication applications for four days in January 2015 for security reasons. Campaigners across the political spectrum embraced digital tools in advance of the city corporation elections in Dhaka and Chittagong, two major cities. There were no reports of state manipulation of online content.

Blocking and Filtering

Domestic websites, including the most popular news sites, ProthomAlo, BDNews24, and Banglanews24, are yet to face any targeted blocking. International social media and communication apps, however, are regular victims of government censorship in Bangladesh. In early 2015, several social network applications were blocked or severely disrupted for four days. Mobile service providers were ordered to block Viber, WhatsApp, LINE, Tango, and mypeople,20 supposedly on grounds that terrorists were using the platforms, which are also used by opposition activists and other internet users. In 2012 and 2013, netizens in Bangladesh also experienced blocks on YouTube and Facebook. During these earlier instances, the blocks appeared to be implemented on a more ad hoc basis. On January 19, 2015, mobile operators reported receiving official, written directives from the BTRC to block ac-

cess to the applications until January 21, when the services became accessible again. No appeals have been documented in response to censorship directives. Such opaque content regulation has resulted in self-censorship by social media users, bloggers, and online news media.

Content Removal

The BTRC censors content relating to religious issues or offending state leaders primarily by issuing informal orders to domestic service providers, who are legally bound through their license and operations agreements to cooperate. Service providers describe official censorship as ad hoc in nature, without proper follow up mechanisms in place to ensure compliance. In addition, online news outlets do not have the government recognition granted to traditional, licensed press organizations, leaving them in a regulatory limbo. International companies are also subject to content removal requests.

In 2013, the government formed an official committee to identify bloggers who had allegedly demeaned the spirit of Islam. The committee participated in discussions with clerics to produce a list of bloggers and Facebook users they alleged had published blasphemous anti-Islamic content. Though there were more than 80 names on the list, the BTRC subsequently directed domestic blog-hosting platforms to close the accounts of just four bloggers it identified as “antireligious elements.” All four were prominently involved in the Shahbag movement, which had come into conflict with ultra-religious groups as well as the administration, which they accused of poor governance. They were subsequently arrested (see Prosecutions and Detentions for Online Activities). The owners of the host platforms reported that officials never used court orders to support the action.

Media, Diversity, and Content Manipulation

Online media practitioners and social media opinion makers reported a climate of self-censorship among social media users, bloggers, and online news media on political and religious topics during the coverage period of this report, which saw fatal attacks on bloggers and several criminal charges in relation to digital activity (see Prosecutions and Detentions for Online Activities). However, no commentators with undeclared sponsorship have been documented manipulating online debate in favor of one side or the other. There were also no documented economic constraints specifically targeting online media outlets imposed by the government or other institutions.

Despite the practice of self-censorship and attacks on bloggers, Bangladesh is still enjoying a vibrant offline and online media industry, and the number of active bloggers is growing. The BTRC has identified 48 active domestic blog hosting platforms, including SomewhereinBlog, Amarblog, and Shocholayoton.

23 Interviews with seven experts who requested anonymity, 2013, Bangladesh.
Digital Activism

The Shahbag movement, which was initiated by the Bangladesh Online Activists’ Network, is the country’s most significant example of online activism to date. The protests coalesced around a February 2013 war crimes tribunal verdict involving a political leader and quickly took on a political element. In its early stages, the movement spread through blogging, Facebook, and mobile telephony. Twitter, use of which had been rare in Bangladesh, gained popularity as a tool to broadcast information about Shahbag. During the coverage period of this study, no comparable instances of online activism took place in Bangladesh. Several groups in the capital, Dhaka, used digital tools to arrange fundraising events to help people affected by severe winter weather in the northern part of the country. The event drew significant participation and received mainstream media coverage as well.

Major political parties significantly increased their online activity during the two major city corporation elections in April 2015. For the first time in the country’s history, netizens used social media to collaboratively develop and circulate populist election agendas among voters and candidates.

Violations of User Rights

The year 2015 saw the most casualties for online activists in Bangladesh on record. Bloggers Abhijit Roy, Washiqur Rahman, Ananta Bijoy Das, and Niladri Chattopadhyay Niloy were fatally attacked, allegedly by religious extremists, in separate incidents in February, March, May, and August of 2015, respectively. In September 2014, a local court sentenced mobile phone user Tonmoy Mollick to seven years in prison under the ICT Act for making parody songs mocking the prime minister and the father of the nation and sharing the song with others. There were at least two other arrests for criticizing or making fun of the prime minister and the government.

Legal Environment

Article 39 (1, 2) of Chapter 2 in the Constitution of the People’s Republic of Bangladesh recognizes freedom of thought, conscience, and speech as a fundamental right. Online expression has been traditionally considered to fall within the scope of this provision. The judicial system of Bangladesh is independent from the executive and the legislative branches of government, but critics say it can be partisan. Police and regulators generally bypass the courts to implement censorship and surveillance without oversight. The Information and Communication Technology Act of 2006 is the primary

30 Faheem Hussain, Zyma Islam, and Mashiat Mostafa, “Proliferation of Twitter for Political Microblogging in a Developing Country: An Exploratory Study of #Shahbag,” Research funded by the Asian University for Women Faculty Research Fund, 2013.
35 “The Historic Masdar Hossain Case and the Independence of Judiciary of Bangladesh: A Compilation,” Wahab Ohid Legal
legal reference for addressing issues related to internet usage, and defining as well as protecting freedom of expression online.\textsuperscript{36} It introduced punishments for citizens who violate others’ rights to communicate electronically: Section 56 of the act defined hacking as a crime punishable by up to three years in prison, a fine of BDT 10,000,000 (US$125,000), or both. However, under Section 57, different types of violations on social, political, and religious issues made electronically are punishable by a minimum of 7 and a maximum of 10 years imprisonment and fines up to BDT 10,000,000 (US$125,000).\textsuperscript{37} Sections 68 and 82 respectively contain provisions for a Cyber Tribunal and Cyber Appellate Tribunal to expedite judicial work related to any cybercrime. The tribunal, to be established in consultation with Bangladesh’s Supreme Court, will be led by a government-appointed judge. The Appellate Tribunal can dissolve the Cyber Tribunal’s verdicts.\textsuperscript{38}

On August 19, 2013, the ICT act was amended and subsequently approved by the cabinet. Far from strengthening the law to protect political speech on the internet, the amendment made prison terms considerably harsher, increasing the maximum prison term to 14 years.\textsuperscript{39} Before the amendment came into effect, police had to seek permission before making ICT-related arrests.\textsuperscript{40} Now no warrant is required, and offences under the act are non-bailable, meaning suspects must apply for bail at a court.\textsuperscript{41} The harsher provisions in the ICT Act may reflect the government’s insecurity regarding internet activism and security.

Prosecutions and Detentions for Online Activities

According to local police, there are around 300 cases being investigated under the ICT Act and 21 cases pending with the Cyber Tribunal, mostly dealing with issues related to social media postings.\textsuperscript{42} In the most significant sentence of the coverage period, a local court sentenced 25-year-old Tonmoy Mollick to seven years in prison under the ICT Act in September 2014. He was on trial for making parody songs mocking the prime minister and the father of the nation and distributing them with his mobile phone.\textsuperscript{43} On August 12, 2015, outside the coverage period of this report, a court in Dhaka sentenced a public university teacher in absentia to three years of rigorous imprisonment, which includes hard labor, in a sedition case filed for making a derogatory comment about the prime minister on Facebook in 2011.\textsuperscript{44}

In July 2014, the police formally charged AKM Wahiduzzaman for making demeaning comments

\textsuperscript{44} ”University teacher jailed for Facebook post on Bangladesh PM,” The Daily Star, August 13, 2015, http://bit.ly/1VNPKXg.
against the prime minister and her family online under the ICT Act. A political activist filed a defamation case against the National University geography lecturer in 2013 for allegedly insulting Prime Minister Sheikh Hasina and her family on Facebook; police filed another case against him under Section 57 of the ICT Act in March 2014. In mid-2015, he was in hiding to escape the charges.

There were at least two instances where people were arrested for criticizing or making fun of the prime minister and the government. On August 2014 Major (Rtd.) Md. Shamsuzzoha, a former army officer, was arrested for making allegedly “provocative” statements on social media against leading politicians, including the prime minister. A case was filed against him under the ICT Act. On September 2014, Imran Hossain Arif was arrested by police for addressing the prime minister as his sister and her son as his nephew, which was interpreted as an insult. He also faced charges under the ICT Act.

Four renowned bloggers, Asif Mohiuddin, Rasel Parvez, Mashiur Rahman Biplob, and Subrata Ashikari Shuvo, were formally charged with harming religious sentiment under Section 57(2) of the ICT Act 2006 after conservative political forces branded them as anti-Islamic atheists (see Content Removal). The cases have been repeatedly put on hold since then.

**Surveillance, Privacy, and Anonymity**

The government allows anonymous access and web posting, and does not require website owners, bloggers, or internet users to register, though citizens must provide their national identity card and related personal information to obtain a mobile connection. However, the amended Bangladesh Telecommunication Act of 2010 allows government mechanisms to intercept electronic voice or data communications from any individual or institution to ensure the security of the state without a court order; the act also requires domestic service providers to cooperate, though without clear provisions detailing procedures or penalties for noncompliance.

After the January 2015 blocking of mobile voice and messaging applications like Viber, there was a popular belief that the government had acquired the capability to monitor the applications while they were inaccessible, though the fears were never corroborated and there were no reports that usage of the applications fell as a result of the rumor. The government made seven requests to Facebook for information on seventeen Facebook users from January to June 2014, but Facebook did not comply.

In April 2014, the UK-based nonprofit Privacy International reported Bangladesh’s Rapid Action
Battalion, a special forces unit implicated in human rights abuses, was seeking to purchase mobile surveillance technology from a company based in Switzerland. The technology would allow police to “indiscriminately gather data from thousands of mobile phones in a specific area and at public events such as political demonstrations,” according to Privacy International. In November 2014, WikiLeaks published information on the purchase of German surveillance software by a Bangladesh law enforcement agency to monitor the country’s digital traffic. A news report published in late 2015, outside the coverage period of this study, documented government plans to invest in surveillance technology to strengthen their oversight of mobile phone, email, and social media communication.

According to Article 43 of the country’s constitution, Bangladesh recognizes its citizens’ right to privacy and correspondence. However, there is no specific privacy or data protection law in Bangladesh, leaving young people vulnerable to privacy violations, predominantly through the voluntarily sharing of information via mobile phones and the internet.

**Intimidation and Violence**

Three individuals were subject to fatal physical violence for online activity in Bangladesh during the coverage period of this report. On February 25, Bangladeshi-American atheist blogger and writer Dr. Abhijit Roy and his wife, Rafida Ahmed Bonya, were attacked by two unknown assailants on the Dhaka University campus, while returning from the annual book fair. Abhijit Roy managed the blog *Mu-to-Mona* (*Free Thinker*) from America, and had returned to attend the fair. Dr. Roy died and his wife was left badly injured. She sustained four head wounds and her left thumb was sliced off. She is now in hiding in the United States. In a Twitter post on the same day, an Islamist organization, Ansar Bangla-7 (also known as Ansar Bangla Team) claimed responsibility for carrying out the attack.

On March 2, 2015, the elite Rapid Action Battalion in Bangladesh arrested Farabi Shafiur Rahman, a radical Islamist known for his threats against Abhijit Roy. Farabi is suspected of sharing Roy’s location, identity, and photographs with various people. On May 3, 2015, the leader of Al-Qaeda in the Indian Subcontinent claimed responsibility for the killing of Abhijit Roy and the other “blasphemers” in Bangladesh.

On March 30, 2015, another blogger, Washiqur Rahman, known for his critical writings about Islam, was hacked to death near his home in Dhaka in an attack that bore disturbing similarities to Abhijit’s. According to the police, three knife-wielding attackers were involved in the assault. Bystanders de-
tained two, both students from Islamic seminaries, at the scene, while the third one fled. The police later charged four people with murder, including the alleged mastermind. 65

On May 12, 2015, another prominent contributor to *Muto-Mona*, Ananta Bijoy Das, was attacked and killed by four masked men armed with machetes in the northeastern Bangladeshi city, Sylhet. 66 Ananta Bijoy was also one of the founding members of Gonojagoron Mancha, the coalition of activists who started the Shahbag Movement in 2013. 57 News reports say he had received death threats from extremists and had tried to leave the country to attend a press freedom event in Sweden, but was denied a visa. On June 8, 2015, the police arrested a suspect in connection with Bijoy's murder. 68

In August 2015, blogger Niladri Chattopadhyay Niloy was killed in his home by four unidentified assailants. 69 The incident took place outside the coverage period of this report, but brought the total number of casualties for online expression in Bangladesh to four in 2015.

The trend of violently targeting bloggers began in 2013. Before blogger Asif Mohiuddin was detained later in the year, armed assailants hospitalized him in January 2013 with serious stab wounds. 70 After his arrest, Mohiuddin reported verbal harassment from other prisoners and believes he remains on a hit list. 71 In February 2013, leading Shahbag activist Ahmed RajibHaider was brutally murdered by suspected religious extremists. 72 Police found a series of posts targeting Rajib and other key figures in the movement on the blog *Sonar Bangladesh*, which the BTRC subsequently blocked. 73 The first of such posts singled out Rajib for his critical stance against religious extremism. On January 28, 2014, police formally charged Mufti Jasim Uddin Rahmani, the head of a radical Muslim extremist group, and seven university students for his murder. 74 The same group is accused of involvement with the attack on Asif Mohiuddin.

This disturbing series of fatal attacks on secular bloggers and the slow pace of investigation by the government have increased security concerns in the online activist community. However, many have expressed their determination to continue writing in the online space. 75

Sexual harassment amplified through the use of Facebook and other social networks was also documented during the coverage period:

---

On October 24, 2014 in Nilphamari, a northern district of Bangladesh, a newly-wed wife was raped by a man while eight others restrained her husband and tied him to a tree. The assault was filmed and the video released on Facebook, and later removed. Charges against nine men were filed, but no arrests had been made as of May 2015.76

On November 2014, a schoolgirl in the city of Comilla was raped and a video of the assault released online. Police filed charges against three people but no arrests had been made by May 2015.77

Facebook was also abused to lure victims. On October 2014, an individual was arrested for kidnapping and sexually assaulting a woman lured in with a fake Facebook page.78 An additional trend of fake Facebook profiles spreading false reports about other people’s personal lives, sexual orientation, or social interactions, was observed during the coverage period. Several cases have been filed in relation to such manipulation. According to Chittagong police, more than 100 complaints regarding the illegitimate use of Facebook were filed in 2014, including 4 cases under the ICT Act.79

Technical Attacks

Cyberattacks on online news sites and blogs have been documented in Bangladesh, though primarily government websites were targeted during the coverage period. ISPs informally organized a Cyber Emergency Response Team to deal with malicious online threats.80

---

78 "Facebook bondhutto, tatporekmashatok, erpordhorshon" [First becoming a Facebook friend, then got kidnapped for a month, and then got raped], BhorerBani, October 21, 2014, [http://tinyurl.com/pbsmvyp](http://tinyurl.com/pbsmvyp).
Belarus

Key Developments: June 2014 – May 2015

- In late December 2014, the Belarusian government passed amendments to the Media Law and other legal measures that significantly expanded the authorities’ ability to restrict critical online content, including imposing intermediary liability for illegal content posted online and the ability to block websites without court authorization (see Blocking and Filtering and Content Removal).

- The government increased blocking of independent media websites to limit citizens’ access to objective information about domestic and foreign developments (see Blocking and Filtering).

- The authorities stepped up their persecution of independent journalists reporting online, particularly through administrative charges against freelance or unaccredited journalists (see Media, Diversity, and Content Manipulation and Prosecutions or Detentions for Online Activities).

- In February 2015, the government issued a directive restricting the use of Tor and other anonymizing tools, announcing their intention to block access to anonymizers and circumvention tools (see Surveillance, Privacy and Anonymity).

Internet Freedom Status

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>Not Free</td>
<td>Not Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>27</td>
<td>28</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>62</td>
<td>64</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 9.5 million

Internet Penetration 2014: 59 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2015 Status: Not Free
Belarus

Introduction

In 2014-2015, as the internet became an increasingly important source of information for millions of citizens, the Belarusian government stepped up their efforts to control and manipulate online content. Amendments to an already restrictive Media Law and several other directives gave the government significantly greater legal grounds to limit citizens’ access to information on the internet and to stifle critical voices online. Most of the legal changes moved the decision-making mechanisms for censorship from the judicial to the executive branch, removing any right to appeal.

During the past year, the government employed a more comprehensive strategy to pressure online media and prevent citizen unrest related to economic woes and an upcoming election. In addition to passing new legislation, the authorities blocked leading news and information websites at different moments throughout the year. The government increased its persecution of independent and freelance journalists, launching more than 25 cases based on administrative charges against those publishing online. It also continues to employ targeted repression to limit online activism and foster self-censorship among online journalists.

At the same time, Russia stepped up its efforts to manipulate media content in Belarus in the wake of its invasion of Ukraine and as part of its information campaign that targets the “Russian World.” Russian propaganda and misinformation have a particularly pernicious impact in Belarus because the Russian language and Russia-based websites dominate Belarus’ online space.

Nevertheless, more Belarusians are moving online and obtaining more news and information from independent websites. Greater and more effective online activism led to increasing numbers of the population participating in and learning about civil society. Activists made further progress in turning online actions into offline initiatives. Despite additional government control and pressure, Belarus’ journalists and activists continued to expand their vibrant and diverse online presence.

Obstacles to Access

Despite several years of economic stagnation and a downturn at the end of 2014, the Belarusian government continued to invest heavily in the country’s internet and ICT infrastructure. The Measuring the Information Society 2014 Report of the International Telecommunication Union (ITU) found Belarus to be among the world’s most dynamic countries in terms of growth of households with internet access, household connectivity, households with a computer, and fixed and wireless broadband penetration. In terms of the ITU’s ICT Development Index (IDI), Belarus climbed from 43rd place in 2012 to 38th in 2013, overtaking Russia as the country with the highest IDI in the Commonwealth of Independent States region.1

Availability and Ease of Access

The number of internet users in Belarus continues to grow. The ITU reported Belarus’ internet penetration rate at 59 percent in 2014, compared to 54 percent in 2013 and just 27 percent in 2009.2 The

---


Belarus

independent organization Gemius reported that more than 5 million Belarusians—70 percent of the population aged 15 to 74—were accessing the internet by the end of 2014, indicating a growth of 66 percent over the last five years. However, the major trend over the last two years has been an increase in daily users, rather than a pronounced growth of the overall online audience. In 2014, almost 73 percent of Belarusian internet users visited social media sites. At least 2.2 million Belarusians were using social networks by the start of 2014.

Since 2010, the proportion of female internet users rose from 48.7 percent to 51.2 percent. The major divide in access is not between rural and urban populations—since some 75 percent of Belarusians live in urban areas—but between the country’s capital and other regions. However, the share of internet users concentrated in the capital city of Minsk had decreased to 29 percent, and the number of users in towns and rural areas had risen to 39 percent, as of December 2014.

More than half of Belarusian households have access to the internet from a home computer. Some 97 percent of the country's companies are connected to the internet. More than two-thirds of Belarusian internet users go online using a high-speed connection. The government reported that 84 percent of households accessing the internet did so using broadband. The fixed broadband subscriber base reached 2.7 million by the end of 2014, with service penetration at almost 30 percent. This figure has increased rapidly since 2010, when Belarus had Europe’s lowest level of high-speed access. Belarus has the highest fixed-broadband penetration in the CIS region, with over 3.6 million broadband ports available.

As of January 1, 2015, Belarus had over 11 million mobile telephone subscribers with a total penetration rate of over 120 percent; the mobile network covered 99.8 percent of the country’s population. The share of smartphones in the mobile market is more than 30 percent.

Numbering only 1.8 million in 2011, the number of mobile internet access subscribers had grown to 4.3 million by 2014, with a penetration rate of about 46 percent. By 2013, one in three subscribers were connecting to the internet via a mobile device. More than 60 percent of Belarusian youth are reportedly using mobile internet. Nevertheless, only 6 percent of page views in Belarus are made via mobile phones or tablets.

The state-run telecommunications conglomerate Beltelecom continued to expand the country’s international internet gateway capacity, which increased from 450 to 770 Gbps in 2014. As of May 2015, Ookla’s Household Download Net Index ranked Belarus 52nd of 200 countries, with an average broadband download speed of 19.85 Mbps. The average broadband upload speed was 16.86 Mbps.
Belarus

which ranked 26th on the index. The mobile download and upload speeds, 8.8 Mbps and 3.3 Mbps respectively, were less impressive, ranking 65rd and 71st, but improved over the previous year. According to Akamai, Belarus’ average internet connection speed was 4.1 Mbps in the fourth quarter of 2014, compared to 2.55 Mbps in 2013. In 2014, Beltelecom added 150,000 new Wi-Fi hotspots in Belarus. It now operates more than 300,000 throughout the country, of which 75,600 are in Minsk.

The cost of broadband access via DSL and cable is generally tied to volume, reflecting the pricing structure that Beltelecom uses when selling bandwidth to downstream ISPs. Volume surcharges do not create a barrier for most users. Currently prices for unlimited internet access from Beltelecom are approximately $5–$45 per month for individuals, depending on the speed. Commercial clients pay about five times more. While mobile phone and internet access prices in Belarusian rubles increased several times in 2013-2014, the amounts remained roughly the same in dollars due to Belarus’ chronic inflation. Prices have not increased significantly since the beginning of 2014.

Internet access has become more affordable in Belarus, and the country’s broadband value index has improved considerably. In June 2014, Belarusians were paying $6.49 per Mbps (47th of 65 countries). By June 2015, the price had dropped to $2.90 per Mbps, which was 27th in cost per Mbps but 47th when taking into account GDP per capita. Mobile broadband is relatively cheaper than fixed broadband, which is still expensive for much of the population. However, both fall below the ITU’s affordability threshold of five percent of household expenditure. Prices do not generally constitute a barrier to ICT uptake. Nevertheless, the download speed in Belarus is lower than in neighboring countries and the cost of services is higher.

While Belarus has two official languages—Belarusian and Russian—the majority of citizens use Russian in daily life. In fact, Russian-language broadcast, print, and online outlets dominate Belarus’ media and information spheres. As a result, a particular feature of the Belarusian internet is its domination by portals, services, and social media sites based in neighboring Russia. Only two or three Belarusian sites are in the top 10 most popular internet sites in Belarus. Most Belarusian media consumers and internet users get their news and information in Russian from Russian sites. This situation has become more problematic since the Kremlin has ratcheted up its propaganda offensive in the wake of the Euromaidan protests and change of government in Ukraine, Russia’s seizure and annexation of Crimea, and the Kremlin’s support for the conflict in eastern Ukraine. Most internet software used in Belarus is in Russian, although some popular software is also available in Belarusian, often due to translation by local enthusiasts.

18 Ibid.
Belarus

Restrictions on Connectivity

The Belarusian government has not imposed restrictions on ICT connectivity or access to particular social media or communication apps permanently or during specific events. However, the authorities possess this capability, since the backbone connection to the international internet is centralized and is owned by the government.

Beltelecom and the National Center for Traffic Exchange, established by the government in 2011, remain the only entities permitted to handle connections with ISPs outside of Belarus. In 2012, the Center for Traffic Exchange replaced Beltelecom in providing access to the points of sharing national traffic (peering). The Ministry of Communications has issued 180 licenses for secondary ISPs, though only about a third of these are currently active in Belarus. The Beltelecom subsidiary Belpak remains the largest ISP; through it, Beltelecom controls 84 percent of the Belarusian internet market. While the government does not limit the amount of bandwidth that access providers can supply, all ISPs depend on the facilities of the state-owned Beltelecom, which allows the authorities to control access speeds for the entire country.

Two decades after its launch in 1994, the Belarusian domain zone (.by, often called the “BYnet”), has more than 116,000 registered domain names. By early 2014, it was the fastest growing country domain zone in Europe. According to legislation passed in 2010, all legal entities operating in the “.by” domain must use Belarusian hosting services, though it is not clear how widely this regulation is enforced.

ICT Market

By mid-2015, there were 64 internet service providers (ISPs) in the country. However, the number of licensed providers has progressively declined since 2010. The largest selection and best quality of internet access is available in Minsk, where some 38 companies offer access through ADSL, ethernet, cable TV, and mobile networks; smaller cities have fewer options. However, all commercial providers must purchase internet access from Beltelecom, the state-owned telecommunications company. In this way, the government maintains control over the telecommunications market. In 2014 the government announced that the National Traffic Exchange Centre (NCOT) would also begin selling internet access to other providers; however, to date the NCOT has kept its prices in line with Beltelecom’s, effectively allowing Beltelecom to maintain its dominance over the market.

Despite inflation and devaluation, prices for internet access in Belarus have remained stable. One possible reason for this price stability is Beltelecom’s alleged practice of flooding the market with

---

28 See Providers, “in all cities of Belarus,” http://providers.by/by-providers/by_cities
underpriced packages. The national operator has expanded its range of promotional deals, which lower prices for internet access by 50 percent for the general population. Experts speculate that Beltelecom is trying to eliminate competition from private operators.30

**Regulatory Bodies**

There is no independent regulator overseeing ICTs in Belarus. There is strong state regulation and involvement in the telecommunications and media market. The Ministry of Communications founded Beltelecom in 1995 and continues to regulate the company, undermining regulatory independence. In addition, the Presidential Administration’s Operations and Analysis Center (OAC), which was initially a subdivision of the State Security Committee (KGB), has the authority to oversee ISPs, conduct online surveillance, and manage Belarus’ top-level domain (.by).31 Other governmental bodies with authority over this sector include the State Telecommunications Inspectorate, the State Control Committee, the KGB, and the Prosecutor General’s Office.

Last year, President Lukashenka instituted personnel changes regarding who oversees the internet. In June 2014, Minister of Information Aleh Pralyaskowski was dismissed. One independent analyst surmised that the decision was made because of his inability to reign in the independent online media and to counter it by improving the state-run online media.32 In July 2014, Aliaksandr Bazanaw, the former director of the Presidential Administration’s Information and Analytical Center, became deputy director of state-run Beltelecom. Bazanaw, who formerly headed the Information and Public Relations Center of the KGB, is now in charge of cooperation with government agencies.

**Limits on Content**

*The Lukashenka government has been sporadically blocking websites since the 2001 presidential election. In 2014-2015, the government resorted to more blocking in an attempt to limit the spillover from the events in neighboring Ukraine and a worsening economic situation at home. New amendments to the 2008 Media Law, which came into effect on January 1, 2015, and other new acts, expanded the state’s powers to block websites whose content threatens national interests and to hold the owners of media sites accountable for “illegal” content, such as extremist information. Additionally, the conflict between Russia and Ukraine has resulted in an increase in Russian propaganda and manipulation of content in the online sphere of Belarus and neighboring countries.*

**Blocking and Filtering**

In 2014-2015, the Belarusian government passed amendments to the media law and other acts that expanded its powers to block websites deemed to be harmful to the state. As a result of these amendments, and in response to a worsening economic and international situation, website blocking increased during the past year. YouTube, Facebook, Twitter and international blog-hosting services remained freely available, however.

30 Ibid.
On December 19, 2014, in the midst of an economic crisis, the Belarusian authorities announced a series of amendments to the 2008 Media Law that allow the Ministry of Information to treat online media in the same way it treats traditional media. The new amendments allow the Ministry to issue warnings, suspend, and file closure suits against online outlets. The Ministry can block access to online sites if two warnings have been issued within twelve months, and the scope for reasons to issue warnings has been expanded. The Ministry can order sites blocked without a warning for posts it deems illegal. According to the bill, the owners of online resources are responsible for illegal content posted, including material considered to be extremist information or “other information that can harm national interests.” Additionally, online reports disputed by any person must be removed the next day and a refutation must be posted in its place. Online broadcast media are required to notify the Ministry at least two days in advance of plans to add or remove a show from their programming. This requirement can potentially be used to censor or block sensitive programs. Limits on foreign ownership of news outlets in Belarus, including online media, were tightened, from 30 to 20 percent.

In addition to their inherently restrictive nature, the amendments include a number of particularly problematic elements. They expanded the types of information considered to be illegal by adding the phrase, “information, the distribution of which can harm national interests of the Republic of Belarus.” This phrase and other provisions are vaguely formulated, subject to broad interpretation, and can be used by officials to stifle critical media. Additionally, hosts can now be held accountable for all comments posted on their websites. Whereas it was up to the courts to decide what internet posts were illegal, the amendments now empower officials to do so. There is no process for appeal. Minister Ananich made it clear that the amended law applied to all media websites accessible in Belarus, even foreign sites and those based abroad.

The process of enacting the amendments was also flawed. The bill was not officially published for public discussion, and independent media experts were not consulted. The government rushed the amendments through parliament; both chambers approved the bill on December 17 and 19. It was only on December 19 that the bill appeared on the government’s legal website, Pravo.by. It was signed into law by President Lukashenka the next day. The amendments took effect on January 1, 2015. The amendments are seen by the OSCE Representative on Freedom of the Media and other media rights experts to pose a major threat to free speech.

Belarus’ economy is tightly linked to that of neighboring Russia, and when Western sanctions and declining oil prices led to a devaluation of the Russian ruble, causing Russia’s economy to head into
a recession, Belarus’ economy followed suit. As Belarusians began losing confidence in their currency in late 2014, the Belarusian government responded to the crisis by blaming the independent media. Three days after the amendments to the Media Law were passed, Minister of Information Li-liya Ananich summoned representatives of non-state and state media to warn them against “inciting panic” regarding a currency collapse. She suggested that all media outlets should work for the good of the country, warning that if they did not, they could be closed down.38

To make its point and preempt public unrest, the government moved to block two types of websites on December 19-20. The Ministry of Trade blocked and ordered the closure of the e-commerce and news platform Onliner.by, the country’s largest online shopping portal and one of its top 10 most popular websites with over 350,000 daily visitors. Simultaneously, the Ministry blocked and legally suspended the operation of 13 other online stores.39 Four more were shut down on December 22. By the end of 2014, some 30 e-commerce shops had been blocked and ceased operations. The sites were accused of violating online trade and consumer protection laws and regulations. With the rapid devaluation of the currency, Onliner.by and the other sites had been listing prices in U.S. dollars, rather than in Belarusian rubles, and were not abiding by government-set price controls. The authorities viewed them as stoking economic panic. As one official explained, the internet stores had greatly contributed to the “galloping jump in prices.”40 One internet expert compared the closure of Onliner.by and other internet stores to “dropping a nuclear bomb on a single house,” adding that the Ministry of Trade had assumed the functions of an economic and political censor.41

To further limit the spread of non-state information about the financial crisis, the government also blocked the leading independent news and information websites Charter97.org, Gazetaby.com, Belaruspartisan.org, UDF.by, 21.by, Zautra.by, Belapan.by and Naviny.by on December 19-20. The blocking continued for at least a week. Several websites were able to circumvent the blocking by changing their IP addresses. In some cases, the new IP addresses were also repeatedly blocked. After a couple of weeks, the large-scale blocking ended as unexpectedly as it began. However, in late March 2015, some providers again began blocking some of these sites.42

Following a forced 23 percent devaluation, the currency crisis abated in early January 2015. As a result of informal negotiations, written appeals, and meetings with state officials, the news section of Onliner.by was restored in the Belarusian domain zone on January 6. One week later, its shopping services were also reactivated, although without information regarding vendors and prices. By March 2015, the e-commerce site had resumed full operations.

On the first day of the blocking of the news sites, Beltelecom issued a statement explaining that the difficulties in accessing some websites in the national segment of the internet were due to alleged DDoS attacks on its data center.43 However, it became clear that the blocking was taking place at

---

Belarus

the level of the backbone provider, since these sites could still be accessed through circumvention tools.44 Owners of the blocked news sites filed requests to Beltelecom and other state agencies seeking explanations, but none admitted responsibility. In its reply to the Belarusian Association of Journalists, the OAC claimed that it took no measures to restrict access to the websites. ISPs reported detecting no malfunctions of communications equipment, the national internet exchange point, or the international switching center. They also blamed the sites’ inaccessibility on a massive cyberattack. The Interior Ministry’s Cyber Crime Prevention Department reported that it had stopped investigating the incident because it posed no “public threat” and possessed no “elements of a civil or criminal offense.” The Prosecutor General’s Office denied any involvement in the blocking.45

According to a leading IT security expert who requested anonymity, the OAC initiated the blocking. The expert speculated that the order to implementers was of a general nature, without specific or detailed instructions, so the blocking appeared haphazard and the authorities could deny involvement. As in the past, basic techniques such as IP filtering and disabling DNS records were employed. It appears that the authorities do not perform regular or automated monitoring of the accessibility of banned websites, and it generally takes several hours for a new IP address to be blocked. To date, no documented instances of deep-pocket inspection (DPI) filtering have been recorded. However, the Belarusian government is reported to have purchased the equipment and software for DPI, but has yet to use it.

The Belarusian Association of Journalists issued a “Statement on the Massive Blocking of Websites,” decrying the blocking and declaring that the Belarusian authorities had de facto imposed a “state of emergency” on information in the country. It pointed out that the blocking had no legal grounds and contravened the country’s international obligations.46 On December 22, the OSCE Representative on Freedom of the Media criticized the blocking and stated that the amendments to the Media Law posed a significant threat to freedom of expression.47

After passing new legislation to further control online activities, the government moved to block additional websites. In January 2015, the Ministry of Information “restricted access” to two unidentified websites, allegedly over content that included obscene language which could harm Belarus’ national interests by threatening “society’s spiritual and moral potential.”48 By May, an official at the Ministry of Information indicated that access to 18 websites was being limited; these sites were allegedly offering drugs, displaying pornography, and using taboo words. The official claimed that the blocking is “in line with European traditions.”49

On February 25, 2015, the Presidential Administration’s OAC and Ministry of Communications issued a joint directive, Ruling No. 6/8, establishing more onerous mechanisms and procedures for

---

47 OSCE, “New regulation and recent blockings threaten free speech on Internet in Belarus, says OSCE Representative.”
restricting access to websites the government considers harmful. According to the directive, which went into force immediately, websites will be blocked if they contain information about illegal drug trafficking or other information that may not be distributed. Websites may also be blocked if their owners fail to correct violations of the Media Law as required by the authorities. The directive allows not only state agencies but also any individual to propose blocking specific websites.

The directive also included some new restrictive elements. It permits blocking access to Tor, proxy servers and anonymizers that allow people to access banned websites without being identified. Internet users typically use anonymizers to circumvent government censorship and reach online resources banned in Belarus, including opposition websites. While experts do not believe that the Belarusian government will be able to completely block access to blacklisted websites, the audiences of these sites are likely to be sharply reduced.

In addition, the OAC is no longer certifying new anti-virus software. Belarusian legislation requires all anti-virus software to undergo a compulsory state certification. In 2014 and 2015, the OAC warned software distributors against selling uncertified software and suspended its sale. Until Belarusian distributors are able to sell licensed anti-virus software, computers and individuals are at greater risk of malicious activity.

In addition to the amendments to the Media Law, several other directives and decrees impacting the online sphere were implemented during the coverage period. In August 2014, the Council of Ministers adopted Ruling No. 810, which established a National Expert Committee to Assess Information Products for Extremist Materials. The Committee works under the Ministry of Information and will “defend public interests from destructive displays in the information sphere.” The committee will be able to request materials, including those from online sources, for examination. The ruling envisages a separate committee in each of the country’s regions. While the committees’ decisions can be disputed in court, independent experts note that their establishment transfers the evaluation of allegedly extremist materials from the judicial to the bureaucratic sphere. They are concerned that the committees will continue the state’s practice of applying the excessively broad interpretation of “extremism” and “extremist” material in existing legislation to political content.

On December 28, 2014, President Lukashenka signed Decree No. 6 “Concerning prompt measures to counteract illegal drug trade,” which, among other provisions, also allocated broader powers to the Ministry of Information and the Ministry of Internal Affairs to block internet sources and restrict users’ online activities. Finally, the Decree obliged all internet hosts to control and analyze all information, messages, and comments posted on their websites, and operators must keep records of users’ online activity. This imposes liability for third-party comments on website owners and creates additional burdens for owners of online sources.
Belarus

In August 2014, the Russian government blacklisted a number of Ukrainian websites, which also became unavailable in Belarus. Belarusians trying to visit those websites saw the following messages: “Access to the website is restricted under the legislation of the Russian Federation” and “The website may contain information prohibited for distribution on the territory of Russia.” The opposition movement “For Freedom” appealed to Beltelecom and the Ministry of Information, asking them to explain why the decisions of the Russian authorities were being applied to Belarusian internet users, and urging them to take measures to restore access to the blacklisted sites.55 Shortly thereafter the websites became accessible again in Belarus.

On August 14, 2014, Belarus’ most viewed opposition website, Charter97, which is based in Warsaw, Poland, was blocked for Belarusian users. The blocking was carried out through the gateway of Belpak (a part of Beltelecom), through which all internet providers connect. The site was accessible only via proxy services. Beltelecom refused to comment on the blocking. The site’s editor-in-chief stated that access to the site had been blocked at the request of the Russian authorities over the site’s pro-Kyiv coverage of the Ukraine crisis. One week earlier, Charter97 had been blacklisted by the main Russian operator, Rostelecom. Earlier in the summer, Rostelecom had briefly blocked Charter97, making the site also unavailable in Belarus. Beltelecom restored access to Charter97 in the afternoon of August 15.56

In May 2015, the Ministry of Information began warning websites, including a number of political and news sources, that they were allegedly violating the newly amended Media Law. Freeregion.info, Radio Racyja, Tuzin.fm (a music portal), the website of the opposition United Civic Party, and the cultural website Kyky received letters indicating that their websites contain some unspecified “violations of the mass media legislation.”57

Under the newly-amended Media Law, a blacklist of websites is now maintained by the Telecommunications Ministry’s State Inspectorate for Electronic Communication, which makes changes to it based on instructions from the Ministry of Information. Only government agencies and ISPs have access to blacklisted sites, which is to be reviewed daily. Any government body can add to the blacklist by informing the Ministry of Information about sites that, in its opinion, violate the law. A website can be blocked by a provider after 24 hours, while it may take the Ministry of Information up to a month to restore access to it once all violations are corrected. The blacklist of restricted websites and procedures for adding websites to it remains unclear, non-transparent and closed to the public. Experts note that the government’s decisions are made arbitrarily, do not require judicial approval, and allow no course for appeal.58

Although different mechanisms of blocking were applied in 2014-2015, the restrictions on internet content were disproportional to the stated aims. If previously the authorities had blocked internet content only during high-level electoral campaigns or rare instances of political unrest, they now

Belarus

seem ready to restrict the flow of information to cope with Belarus’ growing economic problems.\(^5^9\) Many experts concluded that the December adoption of new internet censorship amendments and their almost immediate implementation were a “dress rehearsal” for the 2015 presidential election.\(^6^0\)

Decree No. 60, which came into effect in 2010, remains in force. Designed “to protect the interests of citizens, society and the state in the information sphere,” the decree introduced provisions by which ISPs are required to block access to restricted information, such as pornography and material inciting violence.

In 2010, the Ministry of Telecommunications and the Presidential Administration’s Operations and Analysis Center (OAC) issued a regulation establishing a blacklist of websites whose access should be blocked in state-run facilities and internet cafes.\(^6^1\) A February 2015 decree revised this blacklist. Two of the country’s most popular independent news websites, Charter97.org and Belaruspartisan.org, as well as the website of the Viasna Human Rights Center, Spring96.org, which were on the old restricted list,\(^6^2\) continue to be blocked in state-run facilities. In practice, ISPs seem to be inconsistent in blocking access to these sites; some have blocked access to blacklisted sites without any user requests, while others have ignored the blacklisting.\(^6^3\) ISPs block the blacklisted websites by web address or in combination with IP filtering.\(^6^4\)

Content Removal

To date, content removal has not been broadly used by Belarusian authorities. However, the December 2014 amendments to the Media Law now permit the Ministry of Information to demand the deletion of information the authorities deem illegal, such as information related to extremism or information considered harmful to national interests.\(^6^5\) The amendments require the owners of websites to remove any online report disputed by any person and to post a refutation in its place. If the online publishers do not comply, their websites can be blocked. Website owners are held liable for any illegal content posted on their site, and can also be punished for abusive or “incorrect” comments left on message boards.\(^6^6\) These official decisions are no longer made by courts but by executive bodies, with no dispute mechanism or right to appeal. Even before the new amendments came into force, online publishers threatened with the possibility of a claim of defamation or harm to reputa-

---


64 In December 2012, Index on Censorship conducted field research using a sample group of blacklisted sites to assess the scope of the filtering. The results indicated varying degrees of blocking. While the sites were available via internet cafes in Minsk and through Belarus’ mobile operators, some or all were blocked in places where the state had greater control over the internet connection, such as government buildings and universities. Andrei Aliaksandrau, “Belarus: Pulling the Plug,” (policy paper, Index on Censorship, January 2013) 12-13, [http://bit.ly/1OyOKO6](http://bit.ly/1OyOKO6).


66 Anastasiya Salanovich, “Minister warns of crackdown on websites for “incorrect” comments on message boards.”
tion by state officials, individuals, or companies, often chose to remove controversial materials from their websites before a formal complaint was filed.

The authorities have also used non-legal pressures, such as intimidation, to force the deletion of specific content. In September 2014, Dmitry Daynenko and his student friends uploaded a video to YouTube showing Dmitry taking the charity “ice bucket challenge,” and then challenging President Alexander Lukashenka to do the same. After the video appeared on the opposition website Charter97, Daynenko was summoned by school officials and the police, who threatened to fine everyone involved unless they took the video down.

Several attempts to force the removal of Belarusian content from YouTube originated from Russia in connection with its recent incursions beyond its borders. In August 2014, YouTube blocked “Lobotomy,” a popular documentary about the 2008 Russia-Georgia war by the award-winning Belarusian director Yuri Khaschevatski, with over 400,000 views. The film was blocked on the director’s own YouTube account for an alleged “violation of author’s rights.” When Khaschevatski informed YouTube that the author’s rights actually belonged to him and requested access to his movie be restored, he was informed that the blocking request had been filed by the Russian TV studio Sut’ Vremeni (“The Essence of Time”) headed by Russian ultranationalist Sergei Kurginian. Kurginian had also filed a request to remove another video by the director, which was about Vladimir Putin.

### Media, Diversity, and Content Manipulation

Destabilizing developments in the region over the past year, including Russia’s propaganda campaign regarding the conflict in Ukraine and Belarus’ economic crisis and 2015 presidential election, have had a significant effect on the online media landscape in the country. In 2014-2015, as the internet became an increasingly important source of information for millions of citizens, the authorities stepped up their efforts to influence and manipulate online content. The authorities also continue to use preferential subsidies to favor progovernment media outlets and accreditation requirements to punish freelance journalists and independent media outlets.

Through its selective use of oppressive laws and threats, the government actively promotes self-censorship, which has been a pervasive phenomenon for web-based media, especially state and commercial outlets. During 2014-2015, self-censorship by online journalists increased in response to greater government restriction and repression of independent media. In particular, the new amendments to the Media Law and related legislation have had a chilling effect on journalists and editors. According to the vice chair of the Belarusian Association of Journalists, “the authorities want to force mass media into self-censorship, all the time considering which materials they can or cannot publish.” For example, the news section of the popular portal Onliner.by has switched off the comments function under selected articles that could generate controversial – and therefore dangerous...
Belarus

– comments. However, everyday Belarusian internet users still feel generally safe in expressing their opinions online, despite increased attacks on independent journalists and websites.

Trolling, or the use of inflammatory, extraneous, or provocative messages, is one of the government’s less direct, but nonetheless effective methods of manipulating online content. Since the 2010-2011 protests, the number of trolls and paid commentators has significantly increased on independent websites. Online obscenities and rudeness continue to be a challenge, often making discussions on forums more divisive. As more Belarusian internet users move to social networks, trolls have also migrated to popular online communities.

While it is difficult to prove that trolls are being paid for their services, especially by the government, one can assume that there is some coordination behind their activities given the fact that they are constantly present on popular and influential internet forums and social networks, immediately react to new developments, and frequently work in teams. In the summer of 2014, local authorities and the Ministry of Internal Affairs refused to take up a complaint by Valery Karankevich, who had petitioned the police in the Mahiloou region to identify and investigate a troll who had insulted and libeled him on the website Voskresinfo. In fact, Karankevich, an opposition politician who had been detained previously for political reasons, was himself questioned regarding the contents of the independent site.

In the wake of its invasion of Ukraine and campaign of intimidation in the region, Russia has been waging an “information war” in the so-called “Russian World,” of which Belarus is considered a part. As a result, the Kremlin has stepped up its efforts to influence media content in Belarus. Russian propaganda and misinformation have particularly pernicious effects in Belarus because the Russian language dominates the country’s media landscape, and the most popular websites in Belarus are based in Russia. As a result, Belarusians are heavily influenced by Russian media content.

Following a similar script employed in Ukraine, Russian nationalist online publications and bloggers have aggressively targeted Belarus over the past year. They have denounced the right of Belarusians to have an independent state, criticized the existence of the Belarusian language and culture, demonized the Belarusian democratic opposition and even attacked Lukashenka for his alleged pro-Western leanings and “disloyalty” regarding Ukraine. Russian trolls have also become more active on Belarusian websites and social media pages, and purportedly outnumber Belarusian trolls. The trolls not only attack prodemocratic online forums but seek to influence viewers and manipulate content on Russian-Belarusian issues for partisan purposes.

---

72 For example, this article “Lukashenko: Decree No. 3 will correct the situation,” Onliner, April 18, 2015, http://bit.ly/1X9ppnD, about Lukashenka’s controversial degree fining so-called “parasites” who do not work, was read more than 52,000 times but evidently has no comments. Upon registering, however, readers trying to comment on the article will find the notification that “Comments to this post are not allowed.” For other articles on the same site, comments are allowed and regularly number in the hundreds.


76 Ryhor Astapenka, “How Russian Culture And Media Shape Belarusian Politics.”


Belarus

In addition to manipulating content online, the government is also increasingly using administrative laws to restrict non-state journalists' ability to work, including stringent requirements for accreditation. 79 Journalists, including those publishing online, are not allowed to work professionally if not accredited by the state. 80 Reporters working for media abroad are required to be accredited with the Ministry of Foreign Affairs. However, Western outlets find it difficult to obtain government permission to operate in Belarus, and it remains almost impossible for Belarusians to obtain a permit to work for a foreign media outlet. For example, in January 2015, the Ministry of Foreign Affairs rejected journalist Victor Parfenenko's appeal for accreditation for the eighth time. 81 In practice, Belarus' Media Law makes it impossible for freelancers to work legally in the country. Many freelance journalists have been harassed and prosecuted by the authorities under the charge of not having appropriate accreditation (see Violations of User Rights).

While Belarus' 2009 Law on Information, Informatization and Protection of Information guarantees access to, and the distribution of, information of interest to the public, the government routinely restricts information from independent journalists and the media, including online websites. Some 60 state bodies can classify their information as secret, state officials cannot speak with journalists without the approval of their bosses, and media can only gain information from official press services or state ideological departments. 82

The government controls all broadcast media and more than 600 newspapers and information websites. It continues to influence and determine online content through significant financial support to progovernment media outlets, despite worsening economic woes. For example, in December 2014, as the Belarusian ruble was losing almost 30 percent of its value, the government issued a directive providing financial support for 26 government-controlled newspapers and magazines, and presumably their websites. 83 In May 2015, the government launched a new website, Belsmi, to promote the state-controlled local media and create a more favorable image of the country. Experts have criticized the site for its one-sided content. 84 While the total amount of funding provided to progovernment online media is unknown, the 2015 state budget allocated EUR 60 million (US$73 million) – an increase of approximately EUR 8 million over 2014 – to support all state-run mass media. These funds are used to “collect, prepare and disseminate state orders on official information.” 85 The state also provides preferential advertising (70 percent of the economy is composed of state-run companies) and subsidizes rent and other operating costs.

In contrast, non-state media receive no government subsidies and suffer from a constant lack of funding. The government employs direct and indirect economic pressure to limit financial support for free media, including independent online media outlets, making it nearly impossible for these

79 The Law on Mass Media envisages an authorization-based procedure of accreditation. Moreover, it does not allow the possibility to appeal against a refusal of accreditation. A journalist is forbidden to carry out professional activities, if he or she is not accredited. BAJ, “Comments on Suggestions to Media Law,” January 24, 2013, http://old.baj.by/en/node/19255.
sites to be profitable. Additionally, restrictive amendments to the Law on Public Associations and the Criminal Code that were passed secretly in 2011 made it a criminal offense for NGOs to receive foreign funding. Since most non-state online outlets are run as NGOs, the amendments pose a direct threat to the viability of Belarusian independent media. Additionally, many independent online newspapers suffer from the negative financial impact of their print versions being repressed and economically discriminated against.

Forced to operate in semi-underground conditions and facing constant pressure from the state, independent online media and opposition websites are unable to monetize their growing audiences and popularity. Most independent news websites are at an economic disadvantage because state and private companies are afraid to advertise on them. There is an unwritten rule advising state agencies and companies not to advertise in the independent media, including internet outlets. In some cases, the pressure is more obvious. In February 2014, for example, the founder of the website Orshatut reported that the KGB had warned a businessman that the site was "not quite the right one" and, to avoid trouble, he should remove his advertising. There have also been cases when foreign companies, especially those cooperating with state agencies, have avoided placing ads on independent websites due to political concerns. As a result, even the most popular independent or opposition online outlets generate little or no advertising revenue.

In January 2015, the government introduced a compulsory registration fee ($8) for websites, information systems, and networks in the national internet domain. Additionally, website owners must inform their service providers of any registration information or website status changes within five days or pay additional fees. This requirement introduces additional financial burdens for website owners and hosting providers. Major hosting providers expressed their discontent with new fees and claimed that the fees are unreasonable and contradict regional practice.

These challenges are compounded by Belarus’ worsening economic problems. After anemic growth through most of 2014, structural weaknesses, aggravated by Russia’s economic crisis, led to rising inflation, devaluation, debt, and unemployment. Belarus is experiencing a recession in 2015. All of these challenges are placing additional economic pressure on non-state media. In January 2015, Belarus’ oldest and once-popular web portal, Open.by, closed down due to economic reasons.

Over the past year, greater numbers of Belarusians viewed independent news and information online because they found it to be a credible alternative to the government’s version of developments in the country and abroad. The vast majority of the top 50 news and information websites in the country continue to be either independent or opposition run. Despite two decades of autocratic government, and one of Europe’s most challenging media landscapes, Belarus continues to have a vibrant and diverse online presence. However, in the wake of Russia’s invasion of Ukraine and the

---

87 For details regarding the government’s economic leverage over the independent print media, see Andrei Aliaksandrau and Andrei Bastunets, "Belarus: Time for media reform," (policy paper, Index on Censorship, February 2014) 6-8, bit.ly/13mvPA.
89 Dr. English, "Digital Report Weekly, January 16th, 2015, «Patriotic» and restricted Internet sweeping the region," Digital Report, January 16, 2015, bit.ly/1kpsF7s. For instance, there are no such fees in Russia or Ukraine.
91 Akavita internet ranking site, accessed June 7, 2015, bit.ly/1LoRJe0.
Kremlin’s “information war,” more citizens expressed trust in state-run media than in independent media in 2014, a dramatic change from the year before. By March 2015, however, the level of public trust to both had become approximately equal.92

In 2014, social networks and blogs grew as important sources of independent information in Belarus, driven by a desire for objective information regarding Belarus’ economic problems and the conflict in neighboring Ukraine. Surveys conducted in 2014 indicated that approximately one quarter of respondents had garnered information about developments in Ukraine from social media sites.93 The Russian site VKontakte remains the most popular social network service; as of January 2015, it had 2.5 million real users per week and was among the top 3 most accessed sites in the country.94 By August 2014, the Russian social network Odnoklassniki had more than 1.3 million real users each month.95 The total number of Facebook users in Belarus ranged from 640,000 to 900,000 as of March 2015.96

Comparative analysis of the media communities on popular social networks demonstrate that information posted and shared by independent media is much more in demand than content published by state media. Links from the social network accounts of independent media are actively clicked, shared and discussed by users, while the social network accounts of the state media are lifeless, with almost no comments or cross-posted links, indicating that they cannot compete with their independent counterparts.97 Progovernment websites have few readers, and state officials do not use social networks.98

Belarus has a vibrant blogosphere. Government restrictions on traditional media have pushed independent-minded commentators to launch their own blogs. The most popular blogging platform is LiveJournal. By 2011, Belarusians comprised one of the largest groups on LiveJournal, with over 600,000 users. For Belarusian intellectuals writing in Belarusian and Russian, LiveJournal serves as an alternative media tool for uncensored texts and discussions on social, political and economic issues. The most popular Belarus blogs have over 10,000 followers,99 which is more than the circulation of many independent newspapers. In the past few years, however, LiveJournal has declined in popularity as more commentators have migrated to Facebook and other social networks. Of particular interest in the past year were blogs posted by Belarusians reporting on developments in Ukraine,100 and the case against the “fence blogger” in Brest.101

95  Gemius, “Top 10 Sites,” accessed on March 22, 2015, http://www.audience.by. Since being accessed in March, Gemius has changed its website and these figures are no longer available.
101 Mikhail Lukashevich has been posting political statements on his fence for a decade. In December 2014, the authorities began an investigation into statements on the “political blog” that allegedly defamed President Lukashenka. In March 2014,
Belarus

The primary role being played by independent activist websites and social media pages in Belarus is offering an alternative to the state’s propaganda and misinformation. In terms of accountability, the major players are websites such as those of the Belarusian Association of Journalists and Viasna Human Rights Center, which seek to hold Belarus to its domestic and international human rights obligations. The country’s recurring economic crises have stimulated more online initiatives designed to foster greater economic transparency and accountability. The most popular of these is the Koshtura-da (“Price of the State”) website, which monitors budgetary expenditures.

Because of the repressive nature of the Belarusian government, many political, civic and media activists have chosen or been forced to emigrate over the last two decades. As a result, a number of Belarus’ most popular and influential websites are based outside of the country, in Poland (Charter97, Euroradio.fm), Russia and Ukraine (Belaruspartisan), and the Czech Republic (Svaboda). Nevertheless, the vast majority of these websites’ viewers are based in Belarus.

In addition, some websites with content related to the LGBT community have been targeted by the government, decreasing the diversity of content available online. Gaybelarus.by, the online human rights project conducted by Belarusian LGBTI groups, has been blocked in Belarus, including from private computers and mobile phones, since June 2013. During most of the last year, web browsers indicated that they could not connect to the site when accessed from Belarus. As of June 2015, however, the webpage was accessible again at Gaybelarus.org.

Digital Activism

Digital activism increased over the past year. Online petitioning has become one of the most popular forms of activism in Belarus. Starting an e-petition is often the first step in raising public awareness about an issue and acts as a catalyst for launching a civic campaign. The day after the authorities shut down the popular portal Onliner.by, a petition demanding its restoration was filed on Change.org and generated over 20,000 signatures in less than 48 hours. More than 8,000 people signed an e-petition against the deportation of Elena Tonkacheva, one of Belarus’ leading human rights defenders and the director of Lawtrend – Center for Legal Transformation, which, among other activities, monitors and publishes reports on internet freedom in Belarus. As the deportation case unfolded, the Center was finalizing the results of its annual research, which showed that government websites were failing to meet the requirements of Belarusian legislation. Despite an intensive online and offline solidarity campaign, Tonkacheva was deported from Belarus.

During the last year, social networks were used more often as tools for civic mobilization. Whereas online campaigns in the past rarely resulted in any meaningful offline activism, more recent initiatives have indicated that this may be changing. One example was the campaign to save the independent bookstore Lohvinau. In a situation similar to the accreditation issue (see above), Lohvinau’s attempts to register with the Ministry of Information were rejected six times for political reasons. The authorities opened a criminal case under Article 367, Part 1 of the Criminal Code (libel against the head of state) against Lukashevich. His house was searched, and his brushes and paint were seized. See “Belarus: Man investigated over ‘fence blog’,” News From Elsewhere (blog), BBC, March 11, 2015, http://bbc.in/1wZ8Kud; BAJ, “Mass Media Week in Belarus,” March 2-15, 2015, http://bit.ly/1Oz9T2X.

102 See Center for Legal Transformation (LawTrend), http://www.lawtrend.org/information-access.
Belarus

bookstore was then fined an unprecedented amount of almost one billion Belarusian rubles (about $65,000) for selling books without a license in January 2015. To save the unique entity, civil society launched a solidarity and fundraising campaign using social networks. A virtual flash mob was organized by writers, activists and ordinary readers, who posted photos of themselves online with their favorite book and a promise to donate money, and a challenge to others to do the same. An independent gallery and artists held an online charity auction in support. By March 24, the campaign had raised enough money to pay off the fine. In March, the Ministry of Information granted the bookstore a license to produce and distribute books.

Finally, online activism continues to be important in election years. Since the 2006 presidential election, independent websites, blogs, internet forums, and online communities have played a growing role in educating citizens, informing voters, monitoring the polls, and mobilizing protests against electoral irregularities. In 2010, social networks became an important tool for carrying out solidarity actions and peaceful protests. With the rapid growth of new media, independent online sources were able to compete with state-controlled newspapers, radio, and television during the 2010 presidential election. Independent online media played a growing role in documenting and reporting numerous violations committed by the state during the 2012 parliamentary and 2014 local elections.

Violations of User Rights

In 2014-2015, the Belarusian authorities tightened their control over freedom of expression and the internet through a series of restrictive legal acts, and the government’s persecution of journalists publishing online increased. While extralegal intimidation and technical attacks were infrequent, the UN Special Rapporteur on the situation of human rights in Belarus noted a deterioration of the legal, regulatory and administrative environment for the internet. While the changes are claimed to protect Belarus and its citizens from “destructive foreign influences,” independent experts believe the new curbs to freedom of expression are more likely due to fears of domestic unrest and a Belarusian version of Ukraine’s Euromaidan revolution as the country’s economic situation worsened in the run up to the 2015 presidential election.

Legal Environment

While the rights to freedom of expression and information are guaranteed by the Belarusian constitution, they remain severely restricted and violated in practice. Since 2007, the government has employed a series of repressive laws—mainly defamation laws—that target traditional media to stifle critical voices online.

On January 28, 2015, amendments to Articles 188, 361 and 367 of the Criminal Code came into force.

106 See #SaveLohvinau, www.savelohvinau.club.
108 Smok, “Will Belarus Increase Internet Censorship after December’s Financial Panic?”
These amendments specifically made information distributed via the internet subject to criminal penalties for defamation, defamation of the president, and threats to national security.110

Prior to and after introducing the December 2014 amendments to the Media Law, the authorities sought to make the case for further regulating the internet. They put forth several arguments, the first being national security. To protect the national cyberspace, the authorities declared their intention to work more closely with like-minded allies. In June 2014, President Lukashenka spoke of cooperating with China, which has managed to “create an effective system for the protection of the national cyberspace,” because “the world has already entered into an era of undeclared cyber wars.”111 In September, a parliamentary committee discussed the ratification of a 2013 agreement with Russia which would coordinate responses to “information threats.”112

### Prosecutions and Detentions for Online Activities

A major issue in 2014-2015 was a mounting campaign of harassment and intimidation against Belarusian journalists working for foreign media without accreditation. During the reporting period, more than 25 legal cases were launched against freelance journalists resulting in fines totaling about $8,000.113 Some journalists have been targeted multiple times. In particular, the government is pursuing Belarusian journalists working for two Poland-based media outlets reporting on Belarus: Belsat and Radio Racyja. All of these cases relate to the journalists’ online work. In one of the cases, for example, journalist Larysa Shchyrakova was charged with the “illegal production and distribution of information” under Article 22.9 of the administrative code for an article published on the Belsat website about tax increases for entrepreneurs in Belarus.

The case of Aliaksandr Burakow is indicative of the campaign against unaccredited journalists. The Mahilou journalist was targeted after three of his articles appeared on the Deutche Welle website. On September 16, 2014, police raided Burakow’s apartment. While being questioned, the police assured him that there were no problems with the articles’ contents, but rather that he was an unaccredited journalist working for a foreign media outlet. Ironically, the search of Burakow’s apartment coincided with the visit of Dunja Mijatovic, the OSCE Representative on Freedom of the Media, to Minsk, where she raised the issue of accreditation when meeting Belarusian officials. Her advocacy did not prevent the authorities from fining Burakow BYR 6 million (US$570).114 Speaking earlier on Belarus, Mijatovic had declared: “Accreditation should not be a license to work and the lack of it should not restrict journalists in their ability to work and express themselves freely.”115

The Belarusian Association of Journalists (BAJ) has condemned the government’s persecution of freelancers, calling it pressure that smacks of threats and blackmail. It pointed out that, under the Media

---

Belarus

Law, the legal provision of “illegal production and distribution of mass media products” (Article 22.9), under which the freelancers are being charged, is applicable to media organizations, not to individual journalists. Furthermore, the persecution of the freelancers violates both Belarus’ constitution and its international obligations.116 BAJ has repeatedly appealed to the authorities to codify the status of freelancer in the Media Law, but the Parliament’s Lower House rejected its proposals. In addition to working illegally, freelancers without press credentials have limited access to official sources of information, cannot prove they are journalists if detained, and receive no social benefits for their work.117

In 2014-2015, the government continued the practice of using materials obtained from online sources as “evidence” to punish individuals for alleged offline crimes or misdemeanors. On November 5, International Stand up for Journalism Day, independent journalists and activists in Vitebsk posted a group photo, taken in front of a locally known graffiti work of a bird escaping from a cage, on their Facebook pages. The activists were participating in the 7th annual campaign of the European Federation of Journalists. In the picture, some held paper cut-outs of cages in front of themselves, symbolizing the plight of independent journalists in Belarus. Several weeks later, the participants were summoned by the police, shown the photos from the internet, and charged with participating in an “unauthorized mass demonstration.” Even a bystander, who was walking by and spontaneously joined the photo session, was arrested and jailed for three days in connection with the case. All seven participants were fined for allegedly breaking the law, a judgement that media rights groups found absurd.118 With fines totaling $1,429, journalists called it the most expensive photo session in the history of Belarus’ justice system. The authorities later painted over the graffiti mural.

In recognition of the problematic nature of using online “evidence” to punish alleged offline offenses, the UN Human Rights Committee accepted a complaint filed by human rights defenders from Hrodna for consideration in June 2014. They had been fined for an “unsanctioned demonstration” based on an online photo of them holding a portrait of the human rights defender Ales Bialiatski, who at that time was a political prisoner. The photo had been taken on International Human Rights Day, December 10, 2012, and posted on the internet in January 2013.119

In January 2015, Alena Melnikava, a well-known independent blogger using the pseudonym Stogava, was fined $240 for insulting a public official in the exercise of his duties. As related in her LiveJournal blog, Melnikava was barred from entering a Minsk subway station by a police officer, who accused her of being inebriated. In the emotional post, Melnikava denied the accusation and called the officer a “ment,” a derogatory term for the police. She described Belarus as a “country run by ments” and posted a picture of him. The officer claimed that, as a result of the insult, he was investigated at work and his mother was offended.120

---

Belarus

Surveillance, Privacy, and Anonymity

Belarus employs systematic, nationwide, sophisticated surveillance to monitor its citizens and control critical expression online. All telecommunications operators are obliged to install real-time surveillance equipment, which makes it possible to monitor all types of transmitted information (voice, mobile text message and internet traffic) as well as obtain other types of related data (user history, account balance, and other details) without judicial oversight. Mobile phone companies are required to turn over personal data of their customers at the government's request.

In 2010, President Lukashenka issued a decree introducing the Russian-developed intercept technology SORM (System of Operational Investigative Measures) and allocating resources for online surveillance technologies. SORM enables government surveillance directly via the provider. ISPs were ordered to buy, install and maintain the SORM equipment at their own expense. In 2012, the state telecom operator Beltelecom reported that it had installed SORM on its byfly network. Since late 2011, deep packet inspection (DPI) technology has been in place for network packet inspection and filtering according to content. The Belarusian government also uses Semantic Archive, software developed in Russia that monitors open data—media archives, online sources, blogs, and social networks. It also employs viruses, malware, and spying software to conduct cyber surveillance.

Western firms have reportedly supplied equipment and software that would allow the state to expand its surveillance of citizens. Since at least 2010, the Belarusian authorities have apparently employed mobile telephone surveillance measures.

Given the government's increasing control over the internet, more Belarusians are using proxy servers and other methods to circumvent it. During the past year, Tor use in the country more than doubled; over 8,000 Belarusians are using it. VPN use is also considered to be very popular. In February 2015, however, the Belarusian government moved to ban access to all anonymity and circumvention tools. Under the new ruling, Belarus may attempt to block not only anonymizers and Tor, but also other security tools like the Opera and Yandex browsers that allow access to almost any website in traffic compression mode.

Under a 2014 decree on limiting the sale of illicit drugs, users of any digital wallets available in Belarus (such as Paypal, Webmoney, YandexMoney and other digital payment systems) will no longer enjoy anonymity, as under the new law they must be identified.

In Belarus, there is no judicial or independent oversight of internet or ICT surveillance. ISPs are re-

---

Belarus

required to make remote access to their databases available on demand to government bodies carrying out investigations. There is widespread belief that the internet traffic, text messages, and voice calls of opposition activists are routinely monitored. One expert notes that while the government continues to significantly expand surveillance over the internet, few Belarusians realize the extent of this surveillance and the threat it poses to internet users in the country.131

Beginning in January 2016, all ISPs must collect information about visits to websites by their customers. These records must be maintained for one year. As a result, law enforcement agencies will have access to the private browsing history of all web users in Belarus.132 Since 2007, internet cafes are required to keep a year-long history of the domain names accessed by users and inform law enforcement bodies of suspected legal violations.133 Internet cafes are also required to photograph or film users.134 Restaurants, cafes, hotels, and other entities are obliged to register guests before providing them with wireless access, whether free of charge or paid.135 Belarusian citizens must present their passports and register when buying a SIM card and obtaining a mobile phone number.

The collection and protection of personal data remains problematic in Belarus. Belarus remains the only post-Soviet state that has no proper legislation regulating the privacy of personal data. It has not joined the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.136 In general, independent experts conclude that “Belarusian legislation does not provide a satisfactory basis for the proper balance between freedom and security online.”137

Intimidation and Violence

In the absence of elections and other major domestic political events from June 2014 through May 2015, there were fewer recorded instances of extralegal intimidation and harassment for online activities than in previous years, though they still remained a prominent trend.

In May 2014, unidentified individuals attempted to enter the apartment of Sergei Bespalov, the administrator of “Maja kraina Belarus” (“My Country Belarus”), one of the country’s largest pro-democracy communities on Vkontakte. Several hours later, electricity to the apartment was cut, and unknown persons broke down the doors. Bespalov managed to escape by jumping out of the window.138 That same day his girlfriend and parents were interrogated by the police. At the time of the

131 Jerome Taylor, “Government of Belarus using ‘new tools’ to silence dissent on internet, says Index on Censorship report,” The Independent, January 4, 2013, http://ind.pn/1IQATQPw. Since a majority of Belarus’ internet traffic passes through Russia, which also employs SORM, it is also presumably spied on by that country’s security services, which have close relations with their Belarusian counterparts.
135 Including the user’s name, surname, type of ID, ID number, and name of the state body which issued the ID, as per Art. 6, Regulation on computer clubs and internet cafe functioning, http://bit.ly/1Igo78B.
Belarus

incident, the community page had over 35,000 followers. Since then, its size has doubled. Bespalov remains in hiding and continues to oversee his site.

Raids of online activists' homes and the confiscation of their computer equipment continue to be common forms of harassment. In September 2014, the homes of several members of the opposition youth organization Young Front were searched by the police, who confiscated hard drives and modems under the pretext that pornographic materials were being distributed from their personal accounts on Vkontakte. The activists called the searches and seizures a provocation. That same month, police raided the Mahilou apartment of the independent online journalist Aliaksandr Burakow, confiscating two laptops and flash drives belonging to his wife. Police also searched his parents' home, and confiscated two hard drives there.

In March 2015, police searched the apartment of another Mahiliou independent journalist and local opposition politician, Ihar Barysau, and confiscated his computer, modem and notepads. These actions were part of an investigation launched due to the complaint of a director of a local company, who had accused Barysau and the independent website Gazetarn of libel. Barysau had written and posted a story about the director losing a large sum of money at a casino. During the investigation, police also searched the Mahilou branch office of the Viasna Human Rights Center, since Barysau sometimes used its equipment, and seized three of the Center's computers. Ales Bialiatski, the chairman of Viasna and a former political prisoner, linked these events to a broader campaign in the Mahilou region that aims to intimidate independent journalists and human rights defenders in the run-up to the October 2015 presidential election.

Family members of online activists are also being intimidated and harassed. In addition to the Burakow case above, Aliaksei Zhalnou—son of the prominent and often repressed Babruysk blogger Aleh Zhalnou—was sentenced in June 2014 to three years of restricted freedom for “violence or threats of violence against a police officer.” Aleh Zhalnou records offences committed by traffic police, posting the videos on the internet, and submitting them as evidence with the complaints he regularly files with the authorities. With his father, Aliaksei Zhalnou was a witness to one such incident near an office of the traffic police, where an argument with an officer ensued. Both the blogger and his son were arrested. Several months later, the police captain involved in the accident sued the son and the authorities opened a criminal case against him. One and a half months earlier, his father Aleh had been beaten by unknown people and hospitalized with head trauma. The police did not conduct an investigation. The blogger’s wife was also fired from her job and is facing criminal charges after she resisted when their apartment was being raided. Independent human rights experts believe that the family is being targeted in retaliation for the father’s watchdog blogging activities and in order to silence him through intimidation.

140 “Some computers are given back to Aliaksandr Burakou and he got acquainted with the protocol of violation,” Viasna Human Rights Center, September 9, 2014, [link](http://spring96.org/en/news/73415).
Technical Attacks

Technical violence online is not widespread, but several instances of unusual attacks against independent websites, as well as independent journalists and civic activists operating online, occurred in 2014-2015.

In July 2014, the website of the international consortium Eurobelarus was hacked. For several days, unknown parties published provocative articles with false information about the situation in Ukraine and promoted the content on social networks. When the website’s editors noticed an unusual increase in visitor statistics, which none of the editors had posted, they informed the public about the hacking. The fake articles were written quite professionally and appeared as typical Eurobelarus posts. Moreover, the hackers altered some original articles, distorting their meaning. As a result, Eurobelarus.info was put on a list of suspicious websites compiled by the Russian search engine Yandex. The editorial team of Eurobelarus believes that the attack was caused by the site’s extensive coverage of developments in Ukraine: at the onset of the conflict with Russia, the site had launched a special project, “Events in Ukraine: The View from Belarus.” The source of the attack remains unknown.143

In January 2015, unknown parties hacked the Odnoklassniki social network account of Larysa Shchyrakova, a Homiel-based independent journalist and civic activist who has often been targeted by the government in the past. They posted explicit photos of Shchyrakova taken from her computer, which had been confiscated in 2010 by the KGB. The hacking took place one day before Shchyrakova was to stand trial for her coverage of a November 2014 protest by a disabled activist in Svetlahorsk. Police had charged the journalist with participating in the “unsanctioned mass event.” The harassment is also related to her alleged reporting for a foreign-based news organization without accreditation (see Prosecutions and Detentions for Online Activities). Odnoklassniki’s technical support service has yet to respond to Shchyrakova’s request to delete the stolen pictures from her account.144

While Belarusian criminal law prohibits these types of technical violence, law enforcement agencies rarely pursue such cases; when they do, the investigation is a mere formality. In March 2014, the Investigative Committee opened a criminal case in connection with a hacking attack targeting the independent website Formats. All the content was removed and two defamatory articles about an opposition activist in Mahilou were posted on the site. The independent journalist and website administrator Aliaksandr Burakow filed a complaint with the police and was declared to be a victim in this case. The website has been shut down since the attack. In August 2014, he was informed by investigators that a proxy server and IP addresses located in Sweden and the Netherlands were used to hack his website, that inquiries had been sent to those countries, and that there was “a theoretical probability that those who had done this could be found.”145

In March 2015, unknown parties hacked Hata, a popular portal listing property for rent and sale. The site’s owner claimed that the hackers posted advertisements for illegal drugs and child pornography on one of the site’s pages. Anonymous emails with links to the hacked webpage were sent to the Ministry of Information and Ministry of Internal Affairs. As a result, the Ministry of Information

Belarus

ordered providers to block access to the portal for disseminating information banned by the newly-amended Media Law. Despite the offensive material being promptly removed, the Ministry of Internal Affairs investigated the portal and had one month to make a decision whether to unblock it or not. The authorities did not take into consideration the argument that the site was hacked, perhaps by competitors, since the owner is obliged to protect his website from such attacks. Visits to Hata’s site fell by 30-50 percent in the week following the blocking. Access was restored in April 2015. In an interview, the owner declared that “my example demonstrates how the new Media Law can become a tool in the hands of wrongdoers.”

Brazil

Key Developments: June 2014 – May 2015

• Brazil began implementing the Marco Civil Law, a so-called “Constitution for the Internet,” which was signed into law in April 2014 and ensures privacy protection for users, net neutrality, and several other positive measures. Since its passage, Marco Civil has clarified many issues related to intermediary liability and internet governance, although secondary legislation involving issues such as data privacy was still under public consultation as of mid-2015 (see Legal Environment).

• Strict regulations on permitted speech established in Brazilian electoral law led to the removal and censorship of political content in the lead-up to the October 2014 general elections (see Content Removal).

• Two bloggers were murdered during the coverage period, likely in retaliation for their online journalism, further limiting the space for free speech and investigative journalism (see Intimidation and Harassment).

Population: 202.8 million
Internet Penetration 2014: 58 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2015 Status: Partly Free

Internet Freedom Status

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>30</td>
<td>29</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free
Introduction

After years of debate and revision, Brazil’s highly discussed Marco Civil Law (Marco Civil da Internet), hailed as a civil rights framework for the internet, was signed into law by the president in April 2014. This law, which contains key provisions governing net neutrality and ensuring strong privacy protections and which further touches on regulation for intermediary liability, has received significant international attention as a new type of legislation predicated on ensuring individuals’ rights as they pertain to the internet. Nevertheless, despite boasting some of the most progressive and comprehensive legislation on the rights of internet users, violence against bloggers, criminal defamation laws, restrictions on anonymity, and restrictive limits on content related to elections all continue to limit internet freedom in Brazil.

Over the year since its approval, the Marco Civil Law has begun to be implemented through new regulations and secondary legislation. The Marco Civil “safe harbor” measures for intermediaries via the official establishment of a judicial notice-and-takedown framework have led to clarification on previously murky legal questions concerning intermediary liability for internet service providers (ISPs) and search engines, although a March 2015 ruling left media outlets open to liability for third-party content in their comments sections. The approved legal text has, however, left regulation of some controversial issues pending. Net neutrality, provisions on storage of users’ data by ISPs, and enforcement of new legal breaches are examples of matters that are to be regulated by a future presidential decree.

The regulation phase of Marco Civil has been characterized by high levels of public consultation and democratic participation—elements that were also present in the formation of the original legislation. On January 28, 2015, the Ministry of Justice initiated a public consultation intended to assess citizens’ positions concerning the regulation of the internet and the enforcement and further regulation of Marco Civil. Given the massive volume of new issues being discussed, the duration of this process was extended from the original 30 days to 90; during this time, more than 1,500 internet users who signed in for the discussion accessed the online platform over 25,000 times. Anatel, the telecommunications regulatory agency, and CGI.br, the Brazilian Internet Steering Committee also carried out specific consultations on net neutrality.

Brazil has enacted a handful of initiatives in recent years to expand and enhance broadband and mobile phone usage. With programs ranging from tax incentives for suppliers of information and communications technology (ICT), to the installation of LAN houses (public and private internet access points) throughout the country, to policies fostering internet use in public schools, to the introduction of 4G services in April 2013, Brazil is making concerted efforts to facilitate continued investment in infrastructure and to increase the number of citizens with internet access. The latest surveys carried out by the National Institute of Geography and Statistics (IBGE) show that Brazil has

---

1 Diego Spinola, "Brazil Leads Efforts in Internet Governance with its Recently Enacted ‘Marco Civil da Internet.’ What’s In It for Intermediary Liability?,” The Center for Internet and Society (blog), Stanford University, April 30, 2014, http://stanford.io/1R0h4PH.
Brazil

50 percent of its population online.\(^5\) Despite its notable progress in increasing ICT availability, however, Brazil still faces challenges in its quest to reach internet penetration rates commensurate with its economic wealth.

While internet penetration rates have been increasing modestly, social media interactivity and related activism are taking center stage in Brazil. Issues that have garnered particular interest in discussions on social media over the past year range from increasing public transportation fares to FIFA’s initiatives for the 2014 World Cup (hosted in Brazil), to concerns over security, education, corruption, and public health. In some cases, since the emergence of the Free Fare Movement, online debate has catalyzed real-world street protests.\(^6\)

Brazil still faces challenges to internet users’ rights in distinct areas, such as defamation charges, violence against bloggers and journalists, and an increasing number of internet-related proceedings before domestic courts and governmental bodies. Reporters Without Borders’s often ranks Brazil as one of top five deadliest countries for media personnel in Latin America.\(^7\) In addition to attacks on print and broadcast journalists, two bloggers—Marcos de Barros Leopoldo Guerra and Evany José Metzker—were killed in relation to their journalistic work in Brazil between late 2014 and early 2015.\(^8\)

In their transparency report, Google consistently cites Brazil as one of the countries with the highest number of content removal requests. The number of removal requests also tends to increase around elections, as Brazil’s controversial electoral law prohibits defaming or insulting candidates in the months leading up to an election. During the October 2014 election, the law was used as a justification for almost two hundred lawsuits and numerous content removal requests, frequently contributing to the suppression of legitimate speech within the online environment. Although amendments and regulations introduced to the electoral law in 2013 and 2014 make it slightly less restrictive, the electoral law remains a primary obstacle to internet freedom in Brazil.

Obstacles to Access

Although internet and mobile penetration rates have increased steadily in Brazil, significant disparities in access, including in the ability to purchase data plans, persist, and Brazil has yet to achieve access rates commensurate with its wealth. A new initiative to introduce Internet.org, Facebook’s zero-rating platform, has the potential to improve access to some online content but has also been criticized by digital rights activists who see the program as a violation of net neutrality. Marco Civil requires the Brazilian Internet Steering Committee (CGI.br), a highly respected institution of internet governance experts, be consulted in policy-making decisions related to internet governance and Marco Civil.

Availability and Ease of Access

Despite economic growth in recent years, Brazil’s access rates remain below average compared to

---


Brazil

many North American and European countries. According to the most recent figures from the International Telecommunication Union (ITU) Brazil’s internet penetration rate reached 57 percent by the end of 2014, compared to 51 percent in 2013 and 40 percent in 2009. Various obstacles, such as high prices—a problem that extends to fixed broadband, wireless, and 3G and 4G technologies—limited availability of services, and persistent social inequalities prevent many households from accessing the internet. A significant digital divide and disparities in infrastructure are evident between various geographical regions, as well as between urban and rural areas.

According to the 2015 data from the Brazilian Institute for Geography and Statistics, 31 million households have internet access, accounting for 49 percent of the population. Of these, 98 percent are connected by broadband and only two percent have dial-up connections. Meanwhile, data from the ITU shows a fixed-broadband subscription penetration of around 11 percent at the end of 2014. Mobile broadband connections have also expanded extremely rapidly over the past five years, quickly becoming a dominant means for Brazilians to access internet. As of the fourth quarter of 2014, Akamai measured Brazil’s average internet connection speed at 3.0 Mbps.

Public paid access centers (also known as local area network, or LAN, houses) remain the primary means of internet access for low income Brazilians in many regions, providing access to roughly a quarter of those from the lowest economic brackets. Although household access is becoming the most common means of connection for those with slightly higher incomes, LAN houses remain relevant to digital inclusion in Brazil, particularly in the country’s impoverished northern regions.

Internet growth has been slower than expected, yet mobile penetration has grown significantly over the past five years, increasing from 88 percent in 2009 to 139 percent (or around 281 million phone subscriptions) by the end of 2014. As of April 2015, nearly 149 million users (approximately 53 percent) had 3G services. According to the National Agency of Telecommunications (Anatel), Brazil had 6.8 million active 4G lines by the end of 2014, representing an increase of approximately 417 percent compared to December 2013. Such advanced connections, however, are heavily concentrated in

---

wealthy urban centers, such as São Paulo.20

The anticipated demand leading up to and during the June to July 2014 World Cup greatly accelerated the development of wireless hotspots and mobile technologies supporting 4G services. While national wireless networks are still small compared to other countries—as of July 2015, Anatel registered over one million hotspots within Brazilian territory21—mobile service providers worked to increase the number in the first half of 2014 as a means of accommodating anticipated increases in 3G and 4G network traffic during the World Cup.

Although the development of 4G services would appear to be a positive step in the enhancement of Brazil’s technological capacity, consumer advisory entities are skeptical, contending that 4G service is expensive and is unlikely to live up to its potential until infrastructure is improved. Furthermore, 3G users will have to acquire new handsets to begin using 4G, indicating additional costs for individuals seeking to upgrade to the latest technology.22 The supply of smartphones devices with 4G services has significantly increased since the technology’s implementation in April 2013, but high prices and limited network still constitute challenges.

Brazil’s federal government initiated a number of targeted internet expansion and improvement programs in 2010. One of these initiatives, the National Broadband Plan (Plano Nacional de Banda Larga or PNBL) aimed to triple broadband access by the end of 2014.23 According to statistics from the Brazilian Telecommunications Association, nearly 172 million internet connections were facilitated by broadband in February 2015, representing an increase of 18.6 percent for that year.24 Yet specialists criticized the final PNBL figures: After almost four years, only 1.8 million (7.9 percent) of the 23 million fixed broadband subscriptions in the country were contracted through PNBL. With regard to access by mobile phone, PNBL covered only 0.6 per cent (800,000) of the total 128.5 million individuals who accessed mobile internet.25

The REPNBL, a legal framework establishing tax incentives for the ICT sector passed in February 2013, complements the PNBL and is intended to encourage investment in existing telecommunications networks in order to expand and modernize broadband and mobile internet capabilities and offer internet access to the population at equitable prices, coverage and quality.26 According to recent data provided by the Brazilian Ministry of Communications, by December 2015 this governmental program aims to provide 40 million households with broadband internet access at an average price of BRL 35 (US$10).27


Brazil

New policies have also been enacted to facilitate the sale of mobile phones within the domestic market in an attempt to expand the use of portable devices with 3G and 4G technology. In February 2013, President Dilma Rousseff signed Decree No. 7,981/2013, which amended the REPNBL and established tax incentives for the ICT sector by exempting certain categories of smartphones from taxation, namely those produced with national content, Wi-Fi connectivity, email access, and open source code for developers. The Ministry of Communications and mobile companies have also launched projects in 2015 to improve high-speed internet access in rural areas of the country.

On April 10, 2015, President Dilma Rousseff and Facebook CEO Mark Zuckerberg announced a partnership between the Brazilian government and Facebook aimed at increasing internet penetration by providing free access to a select group of mobile applications in low-income but highly populated areas of the country, as well as free mobile data for these applications. The Internet.org commercial initiative has the potential to increase access, but critics have worried that it violates net neutrality (see Media, Diversity, and Content Manipulation).

Restrictions on Connectivity

The government does not place limits on bandwidth, nor does it impose control over telecommunications infrastructure. There have been no reported instances of the government cutting off internet connectivity during protests or social unrest. Although there was one instance in February 2015 in which a judge ordered the blocking of WhatsApp after the application failed to comply with an information request in a criminal investigation, the order was suspended and the application was never blocked (see Blocking and Filtering).

The backbone infrastructure for the internet in Brazil is mostly privately owned. In 1998, the state-owned company Embratel, which was responsible for the building of that internet backbone, was privatized and acquired by the U.S. company MCI; later, in 2003 it was acquired by the Mexican telecomm American Movil. Over the past decade, private backbone infrastructure, such as that of Embratel, GVT and Oi, has expanded in Brazil.

With the PNBL, however, Brazil intends to expand government owned infrastructure—including the underutilized optic fiber—to allow for low-cost connections. The significant increase in wired broadband subscriptions from 2010 to 2013 is at least somewhat attributable to the expansion of the state-owned backbone. Since the PNBL was initiated, over 612 Brazilian municipalities, which contain around 40 percent of the population, received service from the state-owned Telebras network.

Internationally, undersea cables connect to Brazil from North America and Europe. Brazil has announced plans to create new undersea cable connections with South Africa and the Caribbean, as well as Portugal. Some of the impetus for building these connections is related to a desire to avoid reliance on U.S. infrastructure after revelations of pervasive U.S. spying on Brazilians in 2013.

31 Internet.org changed its name to Free Basics in September 2015.
33 Anna Edgerton and Jordan Robertson, “Brazil-to-Portugal Cable Shapes Up as Anti-NSA Case Study,” eds. Pui-Wing Tam
Brazil

In 2004, the Brazilian Internet Steering Committee (CGI.br) launched an initiative called PTT Metro to create internet exchange points (IXPs) across Brazil, starting with their first IXP in São Paulo. As of April 2013, there were 22 IXPs in operation, covering 16 of Brazil’s 26 states. Currently, Brazil has at least 25 IXPs installed in the country.

ICT Market

Although there are no significant legal or economic barriers for companies competing in the ISP, mobile, or digital technology sectors, the Brazilian ICT market is highly concentrated. As of May 2015, the market share of four large private companies—Oi, NET, Telefonica, and GVT—corresponded to over 87 percent of the country’s broadband market. In January 2014, the Brazilian antitrust authorities approved the merger of Oi and Portugal Telecom into CorpCo. Once the merger is completed, CorpCo is expected to rank as the leading telecommunication company in Brazil and in Portuguese-speaking countries worldwide.

Recent data regarding Brazil’s mobile market indicates that four large private companies—Vivo, TIM, Claro, and Oi (the latter is also among the companies with the largest percentage of the broadband market)—hold 99 percent of market share. Such high market concentration could make it very difficult for other providers such as CBTC and Nextel to compete in the mobile sector. Despite such concentration, Brazil’s mobile industry is the largest market in Latin America.

Regulatory Bodies

Two regulatory agencies oversee Brazilian ICTs: Anatel, the Brazilian telecommunication agency, and the Administrative Council for Economic Defense (CADE), the antitrust agency that is focused on addressing merger reviews and anticompetitive practices in telecommunications markets. Additionally, in 1995 the government created the Brazilian Internet Steering Committee (CGI.br), for the purpose of coordinating and integrating all internet service initiatives in Brazil, as well as promoting technical quality, innovation, and the dissemination of services. Provisions in Marco Civil mandate that the government consult with CGI.br, and in various instances directly involve the Committee, in the policy-making and implementation of Marco Civil processes.

Anatel is administratively and financially independent, and not hierarchically subordinate to any government agency. Its decisions can only be appealed in court. From the Ministry of Communications,

and James Attwood, *Bloomberg Business*, October 30, 2014, [http://bloom.bg/1gOGiDz](http://bloom.bg/1gOGiDz).
41 Marco Civil, art.24, II.
Anatel has inherited the powers of granting, regulating, and supervising telecommunications in Brazil, as well as much of its technical expertise and other material assets. While both Anatel and CGI.br are tasked with ensuring free, fair, and independent operation of ICTs, the General Telecommunications Act (Law No. 9.472/1997) also empowers CADE to issue decisions on matters such as price setting and collusion.\(^\text{42}\) In May 2012, the new Brazilian Antitrust Act (Law No. 12.529 of November 30, 2011) came into force, introducing a pre-merger control regime in Brazil. Under this act, mergers must have pre-approval by CADE before they can proceed. The act also expands CADE’s substantive enforcement power regarding cartel and unilateral business practices that affect competition as well as consumer rights and benefits.\(^\text{43}\)

CGI.br, a multi-stakeholder independent organization created in 1995, counts among its members the founders of the Brazilian internet. Committee members are elected from the government, the private sector, academia, and nongovernmental organizations. The most recent elections concluded in early April 2014.\(^\text{44}\) CGI.br’s contributions include comprehensive and reliable annual reports on internet use in Brazil, funding for internet governance-related research, and the promotion of conferences such as the annual Brazilian Internet Governance Forum, and the international Net Mundial conference, which was organized in Brazil in 2014.\(^\text{45}\) In June 2009, CGI.br declared the “Principles for the Governance and Use of the Internet,” which include the goals of online freedom, privacy, human rights, and net neutrality as a base for the Brazilian information society.\(^\text{46}\) Many of these principles were adopted into Brazilian law through the Marco Civil in 2014.

**Limits on Content**

*Brazilian authorities do not filter or block messages online, nor do there appear to be limits on access to online content, although the country’s strict electoral laws have resulted in allegations of censorship due to their impact on content critical of candidates and other public figures. While content removal requests filed before local courts continue to pose significant challenges to social media companies in Brazil, a notice-and-takedown provision in Brazil’s recently passed Marco Civil Law has clarified the situation for intermediary liability. Brazilians’ use of social media tools for civic action and activism continues to increase, particularly after the intense protests against the prices of public transportation (the 2013 Free Fare Movement), the FIFA World Cup in 2014, and antigovernment protests in 2015.\(^\text{47}\)*

**Blocking and Filtering**

In keeping with the country’s push to modernize and expand access to ICTs, Brazil’s digital information landscape remains largely unrestricted. There are no proven indications that Brazilian authorities


Brazil

are filtering messages or engaging in widespread censorship online, nor do there appear to be limits on access to online content. Brazilians freely gather and disseminate information via the internet and mobile phone technologies. They have access to a wide array of national and international news sources, blogs, social networking platforms, and citizen journalism, the latter of which has proliferated over the past year. Social networks, communication apps, and video-sharing websites such as Facebook, Twitter, and YouTube are freely accessible and widely used in Brazil.

In February 2015, a judge in the Brazilian state of Piauí ordered the blocking of the messaging service WhatsApp—the most popular app in Brazil at the time. The presiding judge in that case had previously sent an order to WhatsApp, which Facebook bought in October 2014, to disclose information relevant to a police investigation of child pornography in the state. After receiving no answer, the judge, referring to Articles 11 and 12 of Marco Civil, which outline a series of sanctions for providers that violate Brazilian Law or rights to privacy, ordered the service suspended nationwide. Although Marco Civil mentions “temporary suspension of activities that are in violation of the law” as one of the possible sanction against providers, many digital rights specialists argue that the judge’s decision was a clear misinterpretation of the law.48 This attempt to enforce Brazilian jurisdiction backfired, and millions of users spent days under the fear that one of the country’s leading messaging services would be completely blocked. The decision was reversed after a few days of national uproar and WhatsApp was never actually suspended, but the event hints at possible unforeseen effects of Marco Civil enforcement.

Another blocking case extensively reported in Brazilian media channels was related to a block on Secret, an application used to share messages anonymously among friends. Since its launch in Brazil, Secret was associated with practices of cyberbullying, privacy violations, posting of porn without consent, and defamation and libel, which generated broad public criticism of the application.49 In August 2014, a Brazilian court issued an interim order for the suspension of the application Secret in the country based on the argument that internet users should not be able to rely on anonymity to infringe privacy and intimacy of third parties.50 After that episode, Secret decided to cease operations in Brazil in March 2015, by removing its application from Google Play and the Apple Store.

Content Removal

Brazilian law continues to limit certain content deemed to be injurious to electoral candidates in the run-up to elections, as well as content that is deemed to be racist or discriminatory. These restrictions on content resulted in the state issuing hundreds of content-removal requests in late-2014 and early-2015. During this same period, a number of court rulings, based on the Marco Civil Law, set precedents on intermediary liability, ruling that intermediaries could not be required to prescreen content but they could be held liable for delays in complying with court orders for content removal. In contrast to these protections for ISPs established during the coverage period, in March 2015, the court ruled that news sites could be held accountable for third party comments on their sites, although as of mid-2015, there were no cases against media companies based on third party com-

State-initiated censorship continues to be an ongoing problem in Brazil in the context of elections. Brazil’s highly controversial Electoral Act of 1997 restricts content that could be viewed as injurious to a candidate, prohibiting such material from publication for three months prior to election day. The law also prohibits campaigning more than three months prior to election day or within 48 hours before or after the election. Although the law historically pertained primarily to offline materials, a 2009 amendment extended its application to the internet and social media platforms, placing restrictions on the online publication of materials pertaining to political candidates.51

Journalists and bloggers who disregard the electoral law are subject to fines and potentially even prison sentences, and electoral courts issue numerous removal requests in order to take down articles or posts that may infringe the law. The electoral law has faced intense scrutiny and public debate particularly because its broad terms harbor the potential to constrain freedom of expression both online and offline. Due to this criticism regarding its restrictions to offline and online speech, Brazil’s Electoral Law was amended in September 2013 to allow for political campaigning on Twitter. However, the law was again amended in December 2013, creating new and specific restrictions to online content concerning candidates and political parties.52

During the 2014 presidential elections, the Superior Electoral Court issued guidelines allowing candidates, parties or coalitions to campaign on their own websites within three months of election day, provided that these websites were reported to the electoral authorities and hosted on servers based in the country.53 Candidates and parties could also create political campaigns on blogs, social networking websites, and instant messaging platforms. According to Guideline No. 23.404/2014, any kind of paid advertising, on corporate sites, with or without profit, and on official or hosted pages by government bodies is prohibited.54

According to the Brazilian Association of Investigative Journalism, 192 lawsuits were filed before electoral courts in several states for suspension or removal of political and electoral related content in 2013 and 2014, with most of the requests being filed around the October 2014 elections.55 For example, in September 2014, a provision of Article 57-D of the recently amended Electoral Act was employed to limit online speech in the Electoral State Court of Sergipe. Several political parties aligned with Eduardo Amorim’s candidacy for the state governorship demanded that anonymous postings against him on Facebook be taken down and a fake profile be excluded from the social network. The Court granted Amorim’s request and based its decision on Article 57-D of the Electoral Law, claiming that the upkeep of such posts would damage the candidate’s reputation.56 In another case, a court ordered the removal of satirical videos from the well-known comedy group Porta dos Fundos because the videos poked fun at the gubernatorial candidate Anthony Garotinho. The videos were only restored to the comedy group’s YouTube channel after the candidate lost in the first round.

52 Such restrictions include liability of servers with regard to early online campaigning; unsubscribing mechanisms for electoral advertising; elevation of fines due to violations of online electoral conduct; and the criminalization of hiring people in order to perform online bashing of candidates. Presidency of the Republic, Civil House for Legal Affairs, Law No. 12.891 of 2013, http://bit.ly/1my5W11.
54 Superior Electoral Court, Guideline No. 23.404/2014.
Brazil

Brazilian law also limits certain content through legislation against cybercrimes. The Azeredo Law (Lei Azeredo, Law #12.735/2012), which pertains to regulation of online content, was approved in April 2013 after major changes to its original, highly controversial proposal. In its final form, the Azeredo Law establishes the creation of specialized teams and sectors structured by the judicial police to combat cybercrimes and to take down racist content (other defamatory content is not directly covered by the bill). Takedowns require judicial notice, but can be issued before police investigations have begun.58

Intermediary liability issues have been settled by the establishment of consistent case law and by new legislation on the matter, with legal certainty created by the Marco Civil Law. Article 18 states: “Providers of internet connection shall not be liable for civil damages resulting from content created by third parties.”59 Meanwhile, Article 19 establishes that application providers will only be held liable for civil damages resulting from content generated by third parties should they refuse to follow a court order requesting specific removal of said content.60 In recent years, case law was slowly built around a similar understanding, with the Superior Court of Justice (STJ) ruling towards a judicial notice and takedown model.61 Exceptions are made for copyright and “revenge porn,” sexually explicit photos or videos distributed without the consent of the individual appearing in them; in these cases a court order is not required for content removal, and the user’s notification alone is enough to make the intermediary liable should it refuse to make the content unavailable in a short time.62

Although ISPs are not responsible for prescreening content, between mid-2014 to early 2015, the Brazilian STJ consolidated a number of precedents ruling that intermediaries are liable for complying with court-issued notice-and-takedown requests within 24 hours.63 Accordingly, in a June 2014 case, the STJ issued a decision obliging Google to compensate a user on Orkut (Google’s former social media site) for moral damages, since the company did not immediately comply with an order to remove defamatory content related to false accounts in her name.64 Although legislation to create a so-called “right to be forgotten,” by obliging search engines to remove links to personal data, has been introduced in the Brazilian legislature, it has not yet been brought up for debate.65

---

59 Law 12.965, “Marco Civil da Internet”, art. 18: The provider of connection to internet shall not be liable for civil damages resulting from content generated by third parties.
60 Law 12.965, “Marco Civil da Internet”, art. 19: In order to ensure freedom of expression and prevent censorship, the provider of internet applications can only be subject to civil liability for damages resulting from content generated by third parties if, after an specific court order, it does not take any steps to, within the framework of their service and within time stated in the order, make unavailable the content that was identified as being unlawful, unless otherwise provided by law.
61 The case law evolved to a notice and takedown model, which means internet providers and content providers were requested to remove the alleged infringing or offensive material within 24 hours upon the judicial order. See for instance STJ, Eduacional/Yahoo, Resp 1.338.214/MT, decision as of November 13, 2013; STJ, Sassaki/Google, Resp 1.338.214/MT, decision as of December 12, 2012.
63 Brazilian Superior Court of Justice (STJ), Appeals to the Superior Court No. 1501187 / RJ (December 16, 2014), 1337990 / SP (August 21 2014); Interlocutory Appeals No. 484995 / RJ, 1349961 / MG (September 16, 2014), 305681 / RJ (September 4, 2009). See: http://bit.ly/1NQa7Tq
64 Superior Court of Justice (Superior Tribunal de Justiça), Appeal to the Superior Court No. 1337990 / SP (August 21, 2014). See: http://bit.ly/1NQa7Tq
Conversely, the STJ ruled in March 2015 that news providers are liable for not preventively controlling offensive posts by its users. The judges held that, unlike technology companies such as Google and Microsoft, news portals have a duty to ensure that their platforms are not used to disseminate defamatory content or violations of the privacy and intimacy of others, since their primary activity is providing accurate information to the public. Although there were no charges against media organizations based on this precedent as of mid-2015, the ruling may encourage online newspapers and other media to preemptively delete their comments sections to avoid liability.

Brazilian requests for content removal issued to Twitter multiplied more than threefold in July to December 2014 compared to the previous period. During this six-month period, Twitter received 27 removal requests from Brazilian courts, 18 of which were related to the general elections in October. The company withheld a total of 101 tweets and 5 accounts from view in Brazil. With the exception of emergency situations or legal prohibitions related to a specific case, Twitter notifies users of requests for account information and restores access whenever it is not forbidden from doing so. Twitter un-withheld 80 tweets and 2 accounts previously found to be in violation of Brazilian election law following the presidential election.

Media, Diversity, and Content Manipulation

Brazilians freely gather and disseminate information via the internet and mobile phone technologies, and they have access to a wide array of national and international news sources. As of June 2014, over 70 million Brazilians had Facebook accounts, representing one third of all Latin American Facebook users and placing Brazil just behind the United States and India in terms of Facebook adoption rates. Brazil is also among the five largest Twitter markets in the world, with the number of users in the country expanding by 26 percent during the last year. Blogs and social networking platforms have become important instruments for citizen journalists and others to access information, defend civil rights, and express political positions.

Although self-censorship is less pervasive in Brazil than in some neighboring countries, the ongoing cases of threats, intimidation, and violence against online journalists and independent bloggers in different regions across the country (see Intimidation and Violence), may indicate that some pockets of self-censorship exist in the country.

The Brazilian federal government has been increasingly engaged in making a stand against human
rights violations online. Within the framework of Marco Civil, the Brazilian Presidency announced on April 7, 2015, the creation of the Pact for Combatting Human Rights Violation Online, comprising a series of commitments intended to promote a safe and discrimination-free virtual environment. This initiative has been supported by Google, Facebook and Twitter, and also includes the institution of an ombudsman for online human rights violations and the launching of a website called Humaniza Redes (Humanized Networks), which will receive complaints on human rights violations and offer internet users instructions on how to safeguard themselves from cyber-violence. The law also has some provisions allowing for the removal of racist or other discriminatory content, which may raise difficult issues about the balance between free speech and combating harassment (see Content Removal). 72

The Marco Civil Law guarantees net neutrality in Brazil. The National Telecommunications Agency (Anatel) initiated a public consultation in December 2014 on the implementation of net neutrality regulation,73 as did the influential private research and digital rights entity CGI.br.74 There is significant debate about what the strong protections of net neutrality in theMarco Civil Law mean in relation to the implementation of zero-rating programs, such as Internet.org, the Facebook initiative that the company is planning to introduce in Brazil.

Facebook claims that Internet.org is an effort to increase global access to the internet,75 but critics have raised concerns that the commercial initiative would provide free access only to a limited number of online applications, including Facebook, rather than to the internet as a whole, with the potential for some users to confuse access with Facebook to access with the internet. Critics argue that Internet.org, and zero-rating programs in general, violate net neutrality principles and stifle competition and innovation by creating "walled gardens" that confine low-income users to certain areas of the internet, giving birth to "cyberspace segregation,"76 and concentrating Facebook’s market share, perhaps to the point of closing out opportunities for other competitors in the future.77 In response to critics, Mark Zuckerberg has argued that limited access is better than no access,78 and in early May 2015, announced the initiative would be open to any app developer.79

Digital Activism

Social media platforms such as Facebook and Twitter continue to play a central role in civic activism in Brazil. Social media has been instrumental to political movements such as the demonstrations against the federal government, which took place in March and April 2015.80 Use of social networks

73 Agência Nacional de Telecomunicações, "Consulta Pública n°3/2015 – Tomada de subsídios sobre a regulamentação da neutralidade de rede, prevista no Marco Civil da Internet."
74 CGI.Br, "CGI.br abre Chamada de Contribuições sobre temas da regulamentação do Marco Civil."
77 Pedro Ramos, "Dilma, Zuckerberg e o fim do Facebook grátis na Claro."
Brazil's Marco Civil Law established a framework for internet users' rights, but other legal provisions—such as criminal defamation laws and laws restricting certain speech during elections—all contribute to a legal environment where individuals can face prosecutions for what they write online. High levels of violence in Brazil's urban centers, coupled with impunity for many crimes, have contributed to one of the highest rates of violence against journalists in the region. During the coverage period, two bloggers and four other journalists were killed.

Legal Environment

Although Brazil adopted some of the most progressive legislation in the world related to internet governance with the enactment of Marco Civil, several competing legal provisions, such as laws criminalizing defamation and blasphemy and restricting speech around elections, remain as obstacles to users' rights online (see Content Removal).

The Brazilian Federal Constitution forbids anonymity but protects freedom of the press and freedom of speech, including cultural and religious expression. Brazil made noteworthy progress in estab-

---

83 From May 2012 to January 2015, the Government received 240,414 requests for information, most of which concerned public administration, finances and economy. From these, the government responded to 239,474 queries, granting the requested information in 175,203. Open Government Partnership Brazil, Mecanismo Independente de Avaliação: Relatório de Progresso 2011–2013, September-October 2013, 54, http://bit.ly/1VcOXOM.
lishing a foundation for internet user rights with the passage of the Marco Civil Law, a so-called constitution for the internet, which was signed into law in April 2014. The groundbreaking legislation establishes the rights to freedom of expression online, offers detailed privacy protections pertaining to personal data, guarantees net neutrality and functionality, and promises to uphold the participatory nature of the internet. Nevertheless, Brazil continued to see instances of local officials bringing charges of defamation—which is a crime punishable by six months to two years in prison or a fine according to the penal code—against bloggers and online journalists. In October 2014, ARTICLE 19, a civil society organization, launched a campaign in Brazil to press for the decriminalization of defamation.

Brazil has a long history of laws that combat discriminatory speech. Although people are rarely charged or imprisoned for racist or discriminatory speech, Brazilian law establishes penalties ranging from two to five years in prison for practicing or inciting discrimination based on race, ethnicity or religion in the media or in other publications. The Azeredo Law, passed in 2012, extended these penalties to online speech. The Criminal Code further outlines punishment for vilifying or mocking religion, with penalties ranging from one month to one year in prison, although it is unclear whether these penalties have been applied online. In July 2015 representatives introduced a legislative initiative to Congress that seeks to increase the penalty for vilifying religion to four to eight years in prison.

In April 2013, a Brazilian cybercrime law commonly referred to as the “Carolina Dieckmann Law” came into force. The law’s adopted nickname comes from actress Carolina Dieckmann due to the fact that the legislation took center stage after nude photos of her were distributed online in early 2012. The law criminalizes breaches of digital privacy such as computer intrusion, the “installation of vulnerabilities,” and editing, obtaining, or deleting information—including credit card numbers—without authorization. The actions of distribution, sale, production, or offer of programs or devices meant to facilitate the aforementioned actions, or to interrupt ICT services, are also categorized as crimes. Associated punishments vary from fines to up to five years imprisonment.

### Prosecutions and Detentions for Online Activities

Several recent court cases concerning defamation may pose threats to freedom of expression online. In April 2014, the blogger Paulo Henrique Amorim was convicted of defamation for insulting...
Brazil

Merval Pereira, a journalist for *O Globo*, whom he called a “bandit journalist.” Although originally convicted to serve jail time, Amorim’s jail sentence was commuted in favor of a fine of ten times the minimum salary to be paid to a public or private social impact institution. Amorim’s lawyer stated that her client will appeal the decision.  

In another defamation case in September 2014, however, a federal judge dismissed a defamation charge against Richard Noblat, a columnist for the *O Globo* newspaper, citing free expression concerns in his decision. The Public Ministry had charged Richard Noblat with racism and defamation for an article published on *O Globo*’s site in which he criticized Joaquim Barboso, the president of the Supreme Federal Tribunal at that time, and implied that Barboso only attained his job because he was black.  

In a previous, more highly publicized case, defamation charges were filed against journalist and blogger José Cristian Góes in December 2012 for a fictional story about the confession of a corrupt colonel that he posted on his blog *Infonet*. The charges, which were both civil and criminal, were initiated by high court judge Edson Ulisses, who claimed that both he and his brother were subject to defamation in the story. It is worth noting that while the story in question mocks political corruption in Brazil, it does not name or describe any particular person. In July 2013, the author was sentenced to seven months and sixteen days in prison. The sentence has since been converted to community service. Góes was also sentenced to pay damages to the judge in a separate civil case, in November 28, 2014. He ultimately decided to shut down his blog on July 22, 2014.

Brazilian courts have also banned individuals from posting online in certain cases. In March 2013, the Civil Court of São Paulo prohibited the activist Ricardo Fraga de Oliveira from posting anything on Facebook about the construction of a real estate development in Vila Mariana, São Paulo, after the real estate company in charge of the development filed a lawsuit against Fraga. Prior to the ruling, Fraga had organized several peaceful protests and a petition against the development. In February 2015, the free speech organization ARTICLE 19 organized a campaign against the continued infringements on Fraga’s right to freedom of expression online. Under slightly different circumstances, the blogger Ricardo Atunes has been prohibited from writing about the criminal case in which he was charged with extortion in 2012, on his social media accounts. The case is still ongoing.

Surveillance, Privacy, and Anonymity

The Brazilian Constitution explicitly forbids anonymity. Although in practice, anonymous speech online is common, judges have occasionally cited the constitution as a basis for limiting particular instances of anonymous speech. For example, a judge in the state court of Espírito Santo cited the constitutional prohibition of anonymity when he issued an injunction on the popular mobile application Secret, which allowed users to post content anonymously. Other judges, however, have held that anonymous posts online are protected as long as it is possible to technically trace the speech through IP addresses and have upheld anonymous speech on the grounds that it is important for free expression and privacy. Secret was ruled permissible in September 2014 based on this argument, yet its developer ceased the application’s operations in Brazil.

Several legal provisions also place restrictions on anonymity. Real-name registration is required in order to purchase mobile phones or open private internet connections, although the use of pseudonyms in discussion forums is a common. Lawmakers have urged further restrictions on anonymity in regard to public access points such as LAN houses, with the suggestion that internet communications be recorded in order to prevent cybercrimes. Legislation of this kind already exists in São Paulo and Rio de Janeiro, and a bill under debate in the Senate (as of June 2015) would require LAN houses to register all users and keep a directory of individual identification for an unspecified amount of time. Perhaps the most restrictive legislative proposal is one introduced in July 2015, which would amend Marco Civil to require users to register their real name and national registration number in order to post on social media or blogs. Although there is little chance that this legal project will be approved, the proposal demonstrates the significant tensions surrounding anonymity in Brazil.

Brazilian electoral law has also been used to request data from anonymous users posting critical comments about candidates. In the State of Rondônia, for example, in July 2014, an electoral judge demanded that Facebook provide an anonymous profile’s personal data in order to identify the user who was posting negative comments and images of the Confúcio Moura, a candidate for governor. Although it is not known whether Facebook complied with this specific request, Facebook’s Transparency Report states that between July and December 2014, the company received requests for data related to 1,967 separate accounts and produced data for 34 percent of these requests. Google and Twitter consistently rank Brazil in the top ten countries worldwide in number of requests for user data, following the United States and Japan.

---

102 “App ‘Secret’, de posts anônimos, chega ao fim, anuncia criador.”
In the first months of 2015, the government opened two public consultations on the regulation and implementation of two pieces of legislation related to users’ rights on the internet: the Marco Civil Law and the Privacy and Data Protection Bill. Marco Civil treats privacy and data protection as fundamental rights, bans the disclosure of users’ personal data to third parties, with the exception of police and judicial authorities, and requires providers to make privacy policies and terms of use clear and understandable. While the Marco Civil is already in effect and regulation is being developed in accordance with the law, the Privacy and Data Protection Bill is in an earlier phase of development. It aims at creating comprehensive data protection legislation establishing clear user rights regarding both government and private sector collection and use of data, and intermediary liability regarding collection, storage and treatment of personal data.

Like similar legislation around the world, such as the EU Data Protection Directive, the bill calls for the establishment of a Data Protection Authority, albeit leaving that creation to further legislation. Unlike many data protection laws in other countries, however, this law specifically mentions internet data protection alongside more general provisions for personal data. On January 28, 2015, the Brazilian Ministry of Justice issued the Preliminary Draft Bill for the Protection of Personal Data (Anteprojeto de Lei para a Proteção de Dados Pessoais) on a website created for public debate. In 2010, a previous version of the Bill was also submitted for online public debate. The new draft is a result of the comments gathered on the first debate and the series of discussions and developments on the issue following the passage of Marco Civil.

During 2014, some evidence emerged that the Brazilian government was increasing its capacity for surveillance. In advance of the World Cup, the government invested US$900 million dollars in security equipment, including some technology such as drones and digital command centers that could be used for widespread surveillance.

**Intimidation and Violence**

Threats, intimidation, and violence against online journalists and bloggers constitute a major restriction on freedom of expression and human rights in Brazil. At least two bloggers and four other journalists were killed during the coverage period, and many other journalists and online activists reported harassment or threats.

On May 18, 2015, police near the town of Padre Paraíso in the Brazilian state of Minas Gerais found the decapitated body of Evany José Metzker, a Brazilian blogger who investigated and wrote about...
corruption, crime, and prostitution for his blog Coruja do Vale. Although investigators have not yet determined that the murder was due to Metzker’s work as a journalist, local news reports suggest that he was engaged in a highly sensitive investigation of a child prostitution ring at the time of his murder.\textsuperscript{114} A few months earlier, in December 2014, unknown gunmen in Ubatuba, a town in the Brazilian state of São Paulo, killed blogger Marcos de Barros Leopoldo Guerra. Guerra had written about corruption of local authorities on his blog Ubatuba Cobra and had received threats in the past.\textsuperscript{115}

Although the Brazilian justice system suffers from a high level of impunity and murders are often left unsolved, convictions in 2015 against the murderers of Déicio Sá, a longtime political journalist and blogger who was killed in 2012, marked a positive development for justice and human rights protection. Sá, who wrote for the newspaper O Estado do Maranhão and ran a blog by the name of Blog do Déicio, was shot to death while sitting in a bar. Police suspect that he was targeted for his reporting. Two defendants in the Déicio Sá case were convicted in a trial by jury on February 5, 2015, and sentenced to 18 and 25 years of imprisonment, respectively.\textsuperscript{116} Another suspect accused of commissioning Déicio Sá’s death still awaits trial.

Bloggers and journalists often face harassment and threats, as well as physical attacks. According to a report from the Brazilian Federation of Journalists,\textsuperscript{117} there were 129 registered cases of violence against journalists in Brazil in 2014. Over 50 percent of such cases occurred while they were covering protests, in the crossfire between the police and protesters. In April 2015, for example, at least five journalists were injured while covering a teacher’s strike in the southern Brazilian state of Paraná, which turned into a violent clash between protesters and police.\textsuperscript{118}

Online bloggers and journalists who work in poor or rural areas and are not linked to major urban media outlets may face more harassment because they lack visibility and the support of colleagues on a national level. Under such circumstances, authorities feel little pressure to solve attacks on the provincial press. Unsolved attacks on journalists may also dissuade provincial reporters from investigating crime and corruption in their regions, resulting in pockets of self-censorship throughout the country.\textsuperscript{119}

Police harassment is also a serious concern in Brazil. In February 2015, the blogger Enderson Araújo received threats from a police officer after writing about young people killed in police shootouts. Araújo, who helped create Mídia Periférica (a blog run by young journalists and focused on poor communities that receive little coverage by the mainstream press), went into hiding after receiving the threats.\textsuperscript{120} In April 2015, several anonymous individuals posted online threats against the photojournalist Fabiano Rocha after he photographed a police officer wearing a mask that covered most

\begin{thebibliography}
\item Committee to Protect Journalists, “Brazilian blogger found decapitated in Minas Gerais state,” May 20, 2015, accessed June 16, 2015, \url{https://cpj.org/x/6104}.
\item “Foi primoroso, diz secretário sobre julgamento do Caso Déicio Sá,” [It was perfect,’ says Secretary about the judgement in the Déicio Sá case] O Globo, February 5, 2015, \url{http://glo.bo/1PxRwIC}.
\item Igor Waltz, “Maioria dos casos de violência contra jornalistas em 2014 ocorreu em manifestações,” [Most cases of violence against journalists in 2014 happened while covering the protests] Associação Brasileira de Imprensa, January 1, 2015, \url{http://bit.ly/1VGDgyY}.
\item Committee to Protect Journalists, “Brazilian journalists injured while covering protests,” May 1, 2015, accessed June 16, 2015, \url{https://cpj.org/x/602d}.
\item Otis, “Bloggers Targeted as Murders Spike in Brazil.”
\item Andrew Downie, “Brazilian bloggers encounter threats online and off,” Committee to Protect Journalists (blog), March 23, 2015, accessed June 16, 2015, \url{https://cpj.org/x/5F6a}.
\end{thebibliography}
of his face during an operation in the Alemão slum.\textsuperscript{121} Brazilian law prohibits unidentified or masked agents from going into the field during peacekeeping operations.

**Technical Attacks**

Although the government has made some efforts to ensure cyber-security, Brazil ranks as the top source and target of cyberattacks in Latin America.\textsuperscript{122} The severity of cyberattacks seemed to increase during the coverage period, with online bank accounts and mobile phones being the main targets. The World Cup and the large influx of foreign visitors to the country are cited as some of the leading reasons why cyberattacks in 2014 incurred significant damage.

In early 2014, Anonymous, a loosely affiliated group of activists and hackers, announced that official websites linked to the FIFA World Cup Games in Brazil would be targeted by future cyberattacks.\textsuperscript{123} The Brazilian chapter of Anonymous followed through on its threats, boasting on Facebook and Twitter about website defacements and DDoS attacks compromising government servers, and providing a running tally listing the number of attacks it had perpetrated against FIFA.\textsuperscript{124} Tiger CEO Emanuele Gentili noted that cyberattacks predicated on damaging Brazilian infrastructure spiked in late April 2014, “with an exponential growth to almost 2,000 daily targets.”\textsuperscript{125} The cyber assault—which grew to include DDoS attacks against government websites, as well as leaks of sensitive information from Rio de Janeiro’s military police—appeared to be coming primarily from outside Brazil, namely from India, Turkey, Europe, Mexico, and the United States.\textsuperscript{126}

While experts agree that in general, too little attention has been given to cybersecurity and related investments in telecommunications infrastructure in Brazil,\textsuperscript{127} Brazilian authorities seem to be making some efforts to increase cybersecurity. Brazil has embarked in a multi-stakeholder debate on implementing its cybersecurity agenda under development since 2008. One of the core outcomes so far was the opening of a National Cyber-Defense Center to protect against technical attacks.\textsuperscript{128}


\textsuperscript{123} “World Cup Threat from Web Activists,” BBC, February 26, 2014, \url{http://bbc.in/1ml6wcZ}.

\textsuperscript{124} Kate Vinton, “Hacktivist Group Anonymous Targets World Cup,” Forbes, June 18, 2014, \url{http://onforb.es/1jeCSvA}.

\textsuperscript{125} Federico Guerrini, “Brazil’s World Cup of Cyber Attacks: From Street Fighting to Online Protest,” Forbes, June 17, 2014, accessed July 15, 2015, \url{http://onforb.es/1qepzc7}.

\textsuperscript{126} Federico Guerrini, “Brazil’s World Cup of Cyber Attacks: From Street Fighting to Online Protest.”

\textsuperscript{127} Carla Modena, “Governo Destina Baixo Orçamento para a Segurança Cibernética,” Jornal Da Globo (blog), Globo, July 27, 2013, \url{http://glo.bo/1LerW23}.

Cambodia

Key Developments: June 2014 – May 2015

- A draft telecommunications law leaked in June 2014 could threaten privacy and anonymity through increased surveillance; a separate problematic cybercrime bill remains pending (see Legal Environment).

- A government working group was established in September 2014 to research mechanisms to restrict access to “immoral” online content (see Blocking and Filtering).

- In July 2014, a journalist was found guilty of defamation online in a verdict observers considered harsh (see Prosecutions and Detentions for Online Activities).

- In a positive development, sharing and discussion online helped prompt a police investigation into the murder of a businessman in December 2014 (see Digital Activism).

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>47</td>
<td>48</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 14.8 million
Internet Penetration 2014: 9 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: No
Press Freedom 2015 Status: Not Free
Introduction

_Freedom on the Net_ rates the internet only partly free in Cambodia, though it remains the country’s freest medium for sharing information. Stringent regulation of traditional media makes the internet an especially valuable platform, providing access to diverse sources of information and allowing users to document human rights abuses, mobilize for protests, and engage in online activism. Although not yet widely accessible—particularly for women, rural populations and poorer people—the internet’s range is nonetheless increasing. Smartphones are proliferating, as is Wi-Fi.¹ Advancements in Khmer script technology have further improved accessibility,² while mobile phone applications have been utilized as a tool for activism, education, health, and agricultural purposes.³

Some concerning developments for internet freedom occurred during the coverage period. A potentially repressive cybercrime law, leaked in draft form in early 2014, remains pending. A separate draft telecommunications law that threatens the privacy and anonymity of internet users through increased surveillance was leaked to the public in June 2014.⁴ This was followed in September by the establishment of a governmental working group, which was tasked with researching mechanisms to restrict access to immoral content online, a mandate that could be abused to censor political expression.⁵ In December 2014, news reports said that the government intends to install surveillance equipment on the networks of internet service providers (ISPs) and mobile phone operators.⁶ Nonetheless, it seems that the widespread implementation of these restrictions and surveillance mechanisms is limited by governmental resources, capacity, and expertise. When the government employed two hackers from the Anonymous Cambodia group, following their conviction for cyber-attacks on government websites,⁷ many saw it as an attempt to increase their information technology know-how.

Even without the systematic application of these measures, existing laws threatened internet freedom in 2014. In one example, journalist Rupert Winchester was found guilty in July 2014 of defamation for an article about a businessman published on his personal blog.⁸ More positively, online interest and criticism of a murder investigation put pressure on the government to arrest the suspects in a murder inquiry involving the business community in December 2014.⁹

---


⁹ Saing Soenthrith and Van Roeun, “Murder ‘Mastermind’ on Run; Parents Arrested,” _The Cambodia Daily_, December 4, 2014,
Obstacles to Access

The proliferation of smartphones has enabled an increasing proportion of the population to access the internet regularly, although its impact has been less felt among women, rural populations, and poorer communities. Advancements in Khmer script applications have further increased access. Popular opposition has thus far proved an effective mechanism against access restrictions periodically proposed by officials for economic or security reasons.

Availability and Ease of Access

Internet penetration was at nine percent in 2014, up from seven percent in 2013, according to an International Telecommunication Union estimate, continuing a small but steady increase from previous years. Local estimates were higher. Average monthly subscription rates are between US$10 and US$20, depending on connection speed, compared to a GDP per capita of US$1036 (US$86 per month). The average download speed is 5.8 Mbps, well below the global average of 18.2 Mbps.

Mobile phone penetration is higher than internet penetration, with a 2014 penetration rate of 155 percent. In a 2014 study conducted by the Open Institute and the Asia Foundation, 94 percent of more than 2,000 randomly selected respondents nationwide said they owned their own phone. Twelve percent said they used more than one phone, and 25 percent used more than one operator. The use of smartphones is becoming increasingly common, and 19 percent of Cambodians report having used their smartphones to access the internet.

Not all citizens have equal access to the internet. Rural areas have less access, although the difference is decreasing due to the increasing availability of wireless broadband. In urban areas, 39 percent of the population own smartphones, compared to 21 percent of the rural population. Wealth also plays a significant role, with poorer citizens having less access. In addition, internet use is less common in older age groups: 44 percent of Cambodians aged between 15 and 25 accessed the internet in 2014 compared to 8 percent of 50-65 year olds. There is also a gender disparity, with 19 percent of women reporting internet use compared to 34 percent of men.19

---

15 Telecommunication Regulator of Cambodia “Mobile Phone Subscribers,” http://www.trc.gov.kh/mobile-phone-subscribers/
Significant advancements have been made in developing Khmer language applications, spurred on by the government’s recognition of Khmer Unicode font as a standard in 2010. Just over half (51 percent) of phones used in Cambodia support Khmer script, though they were more likely to be owned by men (56 percent, compared to 47 percent of women) and in urban areas (57 percent compared to 49 percent). Online translation tools have allowed Khmer speakers to access greater amounts of information in English, and vice versa. The free Khmer Smart Keyboard iPhone app, released at the end of 2014, makes typing in Khmer easier and faster, allowing users to type up to 40 words per minute. In addition, software developed by Alien Dev, a group of young programmers, is capable of converting hard-copy Khmer text to digital documents.

Restrictions on Connectivity

Internet usage has been constrained by poor infrastructure. The absence of an extensive landline network inhibits greater internet penetration, since the fixed landlines which broadband internet services depend on are often unavailable in rural areas. Approximately 98 percent of internet users have wireless access via satellite or Wi-Fi. ISPs develop their own infrastructure, and two have announced plans to construct fiber-optic internet cables. To date, however, neither project has been completed.

Insufficient electricity, often resulting in nationwide blackouts, imposes additional constraints on computer and internet use. Connections can also be extremely slow, especially in rural areas. In recent years, however, mobile broadband has helped boost online activity at such times.

The proposed telecommunications law raises concerns that Cambodia’s Ministry of Posts and Telecommunications (MPTC) could potentially manage communications by establishing a centrally controlled Internet Exchange Point, but details in a draft leaked in 2014 could be subject to change (see Legal Environment).

ICT Market

There were 29 ISPs operating in Cambodia, and 8 mobile service providers as of 2014, compared to 27 ISP providers and 7 mobile service providers in 2013, according to official government figures. In 2013, the MPTC twice tried to set the price of mobile calls, a move observers suspected was de-
signed to protect companies with links to officials from losing out to their competitors. The actions were withdrawn following public opposition, and the market remains competitive.

**Regulatory Bodies**

The Telecommunication Regulator of Cambodia (TRC) was established by royal decree in September 2012. It is mandated with formulating fair and transparent policies, promoting access to quality and affordable services, providing a transparent regulatory process and regulatory guidance, encouraging fair competition and ensuring adherence to international standards and practices. Asides from warning companies it said had failed to pay annual registration fees, the TRC has worked with the MPTC to draft a new telecommunications law, which is loosely worded and has potential to restrict freedom of information.

In addition, government officials at both the local and national level have attempted to limit access to the internet through circulars and announcements. In some cases, popular opposition has overcome these efforts. For example, in 2012 a circular proposed to close all internet cafes within 500 meters of a school. As this would have effectively forced all internet cafes to close, a strong public backlash resulted, and it has not been implemented. During the coverage period of this report, no such restrictions were applied either locally or nationally.

**Limits on Content**

The internet is a valuable platform, not only to access unbiased information, but also to share human rights abuses, mobilize people for protests, and engage in online activism. The Cambodian government has yet to adopt a rigorous, systematic approach to internet censorship, but took a possible step in that direction during the coverage period with the launch of a working group to explore censoring immoral content.

**Blocking and Filtering**

The government sporadically requests ISPs to block certain websites for political or moral reasons. In September 2014, the government formed a working group to look at possible mechanisms to restrict access to immoral content in Cambodia. Restricted content would include pornography, hate speech, and discriminatory language directed toward a political party or its supporters. These ideas are yet to be implemented, and to date, politically motivated blocking has not been systematically applied.

---

35 A circular is a measure endorsed by a minister or the prime minister to explain a point of law or to provide guidance with regards to a point of law. It is advisory in nature, and does not have binding legal force, though it can include penalties for non-compliance.
Blocking is nontransparent and appears to be based on informal communications between ISPs and government officials, which eliminates the possibility of an appeal and makes verifying internet censorship problematic. In 2011, the Minister of Posts and Telecommunications requested that mobile phone operators cooperate in blocking certain websites that impact Khmer morality, tradition and the government, while the Phnom Penh Post leaked the contents of an email sent by an MPTC official to 10 ISPs thanking them for implementing the blocks. In 2011, the popular blog Khmerization was unavailable for some periods on some ISPs, as was a report by the UK-based NGO Global Witness in 2009. YouTube, Facebook, Twitter and international blog-hosting services are freely available.

Content Removal

The scale of content removal is difficult to assess, since it is unofficial and nontransparent rather than legal or administrative. There have been instances when internet users have been questioned by police and coerced into removing the content, indicating a tendency for some powerful people to use their influence to force removal of negative comments about them online. In 2013, teacher Phel Phearun was questioned after he posted details about his encounter with Phnom Penh traffic police on Facebook. Separately, marketing manager Cheth Sovichea was detained for a day after accusing local officers on Facebook of confiscating unregistered motorcycles to solicit bribes. He avoided charges by removing the offending post and publically apologizing.

Media, Diversity, and Content Manipulation

The fear of repercussions for sharing political views means that self-censorship remains common among many Cambodian bloggers and social media users. There is no evidence that partisan interests manipulate online information, despite the use of the internet to abuse political opposition during the 2013 elections. There are fears that the CPP will restrict political expression online in the future.

All of the key media organizations in Cambodia have comprehensive websites with access to broadcasts, articles and videos. They also use social media platforms to disseminate information. This is true not only for government-controlled media, but also for independent and English-language media such as The Cambodia Daily and The Phnom Penh Post, helping users to retrieve unbiased infor-

mation. In a positive move, many government institutions, parliamentarians and government officials are using social media, providing easily accessible information to the public.

Digital Activism

The proliferation of internet access has facilitated mobilization among Cambodian youth, who frequently engage in online advocacy activities, including petitions, blogging and hacktivism.48 Telecommunications played a central role in the 2013 national elections. Not only did it provide access to up-to-date information for an increased audience, but Facebook was also used by the opposition to coordinate rallies and circumvent strict media controls. This trend continued in the aftermath of the election when evidence of alleged voter fraud was spread through social media. Additionally, footage of the violent suppression of antigovernment protests in January 2014 has helped activists to dispute the state media’s portrayal of those events.49 In December 2014, following the murder of a prominent businessman in Phnom Penh,50 online criticism of the police response helped spur the investigation, which led to the arrest of the suspects.

Phone applications have also been utilized to assist in activism and mobilization. For example, VoterVoice allows users to quickly organize campaigns,51 while the application Verboice—a free open-source tool that makes it easy for anyone to create and run projects that interact via voice, allowing users to listen and record messages in their own language and dialect or answer questions with a phone keypad—has been modified in various ways to provide verbal contraceptive reminders,52 provide farmers with information about rice seeds,53 and assist in educating children.54 The Empowering Clogher Project developed the IT and communications skills of female bloggers (cloghers) to enable them to create their own online forums to discuss and share ideas, and advocate for human rights and social change, particularly relating to their own experiences as young women from Cambodian provinces.55

Violations of User Rights

A draft cybercrime law leaked in April 2014 remains a central concern for internet freedom activists. Although not yet passed, the law could criminalize a number of ill-defined activities, introduce harsher punishments for online slander than for the offline version of the same crime, and allow prosecutors rather than judges to order the retention of computer data for criminal investigations. A draft telecommunications law leaked in June 2014 also threatens the privacy and anonymity of internet users through increased surveillance. In addition, it was reported in December 2014 that the government in-

---

tends to install surveillance equipment on the networks of ISPs and mobile phone operators in Cambodia, though it appears that the government’s technical capacity to implement these plans is still lacking.

Legal Environment

The Constitution of Cambodia not only provides for freedom of expression and freedom of the press under Article 41, but it also supports the provisions outlined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which both guarantee those rights. In practice, charges of criminal defamation and incitement as provided by the 2010 penal code are often used to restrict these freedoms.

A pending cybercrime law represents a significant threat to freedom of expression on the internet. The drafting process has been characterized by a lack of transparency and civil society involvement. In April 2014, the freedom of expression advocacy group Article 19 obtained a copy of the Cybercrime Law Draft V.1 and published an unofficial translation. That version prohibited publications "deemed to generate insecurity;" "deemed damaging to the moral and cultural values of the society;" those considered to undermine "the integrity of any governmental agencies;" or those considered "manipulation, defamation and slanders [sic]." The draft carried potential prison sentences of one to three years and fines ranging from KHR 2 to 6 million (US$490 to US$1,480). By contrast, offline slander is punishable by a maximum of one year behind bars.

The lack of adequate definitions in the draft was especially concerning considering the proposed make-up of a National Anti-Cybercrime Committee to enforce it, consisting of high-ranking members of government under the chairmanship of the prime minister. The draft would further grant prosecutors, rather than judges, authority to issue court orders to preserve computer and traffic data for purposes of criminal investigation. The law was reportedly put on hold in late 2014, but in late May 2015, the minister of post and telecommunications announced that it is still under consideration, including criminal sanctions for "people with bad intentions" who "criticize the government."

The draft telecommunications law, which was similarly leaked later in 2014, also provides for governmental control over the management of internet infrastructure and services, giving the state undue influence over telecommunications providers. The draft appeared to authorize the MPTC to install a central Internet Exchange Point to better control communication. Other provisions may be detrimental to individual privacy and criminalize online content perceived as critical of the ruling party.

These developments took place against a broader movement to limit civic participation. In April

2015, Prime Minister Hun Sen and other senior lawmakers said they planned to adopt a highly controversial Law on Associations and Non-Governmental Organizations (LANGO) without consultation.64 No draft has been made public since 2011, with the intention of excluding civil society from the law-making process, despite the fact that it would severely affect their ability to carry out their role. In January 2015, the government announced its intention to introduce a state secrets law that could include criminal penalties for those who leak draft laws for public comment.65

**Prosecutions and Detentions for Online Activities**

Provisions on criminal defamation and incitement from the 2010 penal code have been used to harass and discourage bloggers, Facebook users, and journalists.66 On July 24, 2014, a court in Phnom Penh found journalist Rupert Winchester guilty of defamation for a June 2013 article about a businessman published on his personal blog. In a trial and verdict the freedom of expression community called disproportionately harsh, he was fined KHR 8 million (US$2,000) and ordered to pay KHR 100 million (US$25,000) in damages.67

There have been other convictions involving internet use in recent years. In 2010, Seng Kunnaka was sentenced to six months imprisonment and a fine of KHR 1 million (US$250) for “incitement to commit a felony” under Article 495 of the new penal code, after he printed articles from the KI-Media website for a handful of colleagues.68

**Surveillance, Privacy, and Anonymity**

Although surveillance of citizens’ digital activity is not widespread or technologically advanced in Cambodia, there have nonetheless been a number of attempts to monitor online activity. In 2012, a circular from the Ministry of Interior and the MPTC ordered internet cafes to install surveillance cameras, and phone shops and telecommunications operators to register subscribers’ identification documents on the basis that these measures would “better promote protection of national security, safety and social order”.69 In addition, the circular required used data to be stored by the operators for six days so that designated officials can use the information for investigations of offenses related to “issues of national security, safety, and social order”. The draft telecommunications law has potential to further increase surveillance and erode privacy and anonymity, by establishing a government-controlled Internet Exchange Point allowing centralized oversight of online traffic, among other measures.70

In December 2014, it was reported that the government plans to install surveillance equipment on ISP and mobile phone networks. A senior Interior Ministry official explained that it is important to

---

“strictly control people using the internet and mobile networks.” This development came shortly after the TRC ordered 12 mobile phone operators and ISPs to cooperate with police in an October 2014 letter. Despite these plans, it appears that the government does not yet have the necessarily equipment or sufficient funds to start systematic surveillance.

Also in late 2014, the Council of Ministers’ Press and Quick Reaction Unit announced the creation of a “Cyber War Team,” with the stated aim of monitoring all online activity to “protect the government’s stance and prestige.”

**Intimidation and Violence**

The internet is often used as a medium for threats and intimidation, though there were no incidents of physical violence in retribution for online activity documented during the coverage period of this report. In December 2013, members and leaders of the main opposition Cambodia National Rescue Party (CNRP) were sent threats containing pictures of a gun and ammunition via Facebook. The former leader of the Cambodian Center for Human Rights, Ou Virak, was also targeted online following his criticism of the CNRP’s leader’s use of discriminatory language about Vietnamese immigrants.

**Technical Attacks**

Technical attacks often go unreported in Cambodia, although there has not been any systematic targeting of civil society groups or government critics by hackers. During the 2013 election there were numerous technical attacks, including on government websites. In September 2013, following the elections, the hacking group Anonymous Cambodia, part of the global Anonymous collective, posted a declaration of online war against the Cambodian government following the fatal shooting of a bystander, Mao Sok Chan, at a protest. Several governmental websites were subsequently disabled for short periods of time, and five alleged members of the hacking group were arrested.

---

Key Developments: June 2014 – May 2015

- In January 2015, the Canadian Radio-television and Telecommunications Commission (CRTC) issued a ruling grounded in the principles of net neutrality which stated that telecommunication companies cannot set rules or prices that favor their streaming services over those of competitors (see Media, Diversity, and Content Manipulation).

- In June 2014, a court in British Columbia issued a decision, which was subsequently upheld by an appeals court, requiring Google to remove search results for a copyright-infringing company on all of its domains, not just Google.ca (see Content Removal).

- The government passed two laws, the Digital Privacy Act (Bill S-4) and the Protecting Canadians from Online Crime Act (Bill C-13), which have significant implications for Canadian internet users’ right to privacy (see Surveillance, Privacy, and Anonymity).
Editor’s Note

The following chapter covers developments in Canada through May 31, 2015. In June 2015, the Canadian parliament passed Bill C-51, also known as the “Anti-terrorism Act, 2015.” This law caused significant controversy due to its vague wording and provisions that could have a negative impact on freedom of expression and the right to privacy. However, since the law was passed outside of this report’s coverage period, it did not have an impact on this year’s scores.

Introduction

Internet access in Canada is reliable and affordable for a majority of the population and is generally free of government restrictions. Canadians enjoy strong protections for freedom of expression, as well as a well-developed set of rules regulating intermediary liability in cases of copyright infringement.

Despite these strengths, there remains considerable unease among many Canadians with respect to online rights. Legislative reforms involving privacy protections and surveillance have generated some controversy, with many Canadians concerned about plans to expand the scope for companies to make voluntary disclosures of personal user information without court oversight. While the Canadian Radio-television and Telecommunications Commission (CRTC) issued a positive decision with regard to protecting net neutrality, the Canadian courts have issued several rulings that could increase intermediary liability and restrict access to information.

Obstacles to Access

There are very few infrastructural or regulatory obstacles to internet access in Canada. The internet and mobile phone penetration rates continue to grow, although there are still some barriers related to the affordability of internet access.

Availability and Ease of Access

According to the International Telecommunication Union, the internet penetration rate in Canada reached 87 percent in 2014, compared to 86 percent in 2013 and 80 percent in 2009.1 Canada had a mobile phone penetration rate of over 83 percent in 2014.2 Mobile carriers have deployed a number of newer technologies to provide mobile broadband service, including HSPA+ and LTE.

The government and the Canadian Radio-television and Telecommunications Commission (CRTC), an independent public regulator for the telecommunications sector, have different broadband targets. The CRTC’s 2015-2016 Priorities and Planning Report seeks to provide 100 percent of the population broadband access at speeds of 5 Mbps download or higher by the end of 2015, while, the government has set relatively low speed goals and a longer time frame in a plan that would still leave three-quarters of a million Canadians without access. Industry Minister James Moore promoted the

---

government’s commitment to broadband access in the summer of 2014 with “Connecting Canadians,” a program to bring internet access to 280,000 Canadians who currently do not have access or who have access at speeds considered to be too slow. According to a government release, by 2017 the $305 million investment would extend access at 5 Mbps to 98 percent of Canadian households. However, according to Industry Canada’s recently released 2015-2016 Report on Priorities and Planning, the target date for providing the 280,000 Canadians with new or faster access is now March 2019.

While internet access is widely available in Canada, there is a gap in access related to income: the highest income bracket has a penetration rate of nearly 95 percent, while the penetration rate within the lowest income bracket is closer to 63 percent. Use of public access points such as libraries is declining but is still an important resource, particularly for younger Canadians or those with lower household incomes. Additionally, there is a wide range of content available in both of Canada’s official languages (English and French) as well as many other languages.

Restrictions on Connectivity

There are no government restrictions on bandwidth, although access providers frequently offer services with caps on bandwidth that result in increased fees for users who exceed the limit. The government has not centralized the telecommunications infrastructure in Canada. However, given the vertical integration of the Canadian marketplace, the telecom infrastructure is controlled by a small number of companies, which in theory could facilitate greater control of content and the implementation of surveillance technologies.

ICT Market

To operate as a Canadian telecommunications carrier, a company must meet the requirements in section 16 of the Telecommunications Act. In 2013, Canadian telecommunications revenues amounted to $44.8 billion. The five largest telecommunications companies, five largest cable companies, and five largest independent resellers captured 97 percent of total industry revenues.

Canadians have a choice of wireless internet providers, all of which are privately owned. There are at least three providers to choose from in all markets. Restrictions on foreign investment establish some controls, though Canada has seen some foreign companies enter the marketplace in recent years. The provision of access services is subject to regulation with rules on tower sharing, domestic roaming agreements, and a consumer regulator to address consumer concerns.

For wireless services, three companies dominate the market: Bell, Telus, and Rogers. Those same companies are leaders in the provision of internet services, along with Shaw, Cogeco, and Videotron. The government’s minister of industry, James Moore, has continued to emphasize the need for more competition in this market, using a spring 2015 spectrum auction to provide new entrants with advantages in the acquisition of new spectrum.

---

Regulatory Bodies

The Canadian Radio-television and Telecommunications Commission (CRTC), the regulatory body that oversees the communications industry, operates largely independently from the government. The government appoints the CRTC chair and commissioners. There is no public consultation on the appointment. The government also has, in some cases, provided guidance on their policy expectations regarding telecommunication regulations. Moreover, CRTC decisions can be appealed to the courts, or a government review can be requested. The government has (on rare occasions) overturned CRTC decisions and directed it to reconsider the issue. For example, the government required the CRTC to reconsider its approach to usage-based billing for internet services in 2011.5

Limits on Content

The Canadian government does not generally block websites or filter online content. Illegal content may be removed by legal action taken through the court system.6 YouTube, Facebook, Twitter, and international blog-hosting services are freely available. However, there have been several court cases in recent years that have had negative impacts on intermediary liability, which could have the effect of increasing censorship.

Blocking and Filtering

The government does not generally block or filter online content, and there are few legal mechanisms that may lead to the blocking or removal of online content in Canada. Canada’s largest ISPs participate in Project Cleanfeed Canada, an initiative that allows ISPs to block access to child pornography images that are hosted outside of Canada (as opposed to content hosted within Canada, which is subject to removal).7 Accessing child pornography is illegal in Canada under section 163.1(4.1) of the criminal code.8 The initiative is targeted at international sites that the Canadian government does not have the jurisdiction to shut down.

Under Project Cleanfeed Canada, an individual may issue complaints about content to the ISP or directly to Cybertip.ca, the national tipline for reporting exploitation of children, which will assess the site and, if necessary, obtain an independent, binding judgment from the National Child Exploitation Coordination Centre.9 An appeals process has also been put into place for cases in which content providers believe that their content has been wrongly blocked, although the list of blocked sites is not public since it would essentially provide a directory of child pornography.10 The project blocks approximately 1,000 child pornography images each year.

In April 2015, the government of Quebec announced plans in its budget to require ISPs to block access to online gambling sites. The list of blocked sites will be developed by Loto-Québec, a gov-

---
8 Criminal Code, RSC 1985 c C-46 s 163.1(4.1).
9 OpenNet Initiative, “United States and Canada Overview.”
ernment agency. This is expected to act as a revenue-enhancing measure for the government by directing gamblers to the state government’s own Loto-Québec-run online gaming site, Espacejeux. A November 2014 report found that Espacejeux was not meeting revenue targets, due to the popularity of other sites. The government believes that the website blocking will increase revenues by $13.5 million in 2016-17 and $27 million per year thereafter. The plan is likely to face a legal challenge, both on free speech and jurisdictional grounds, since the federal government has exclusive jurisdiction over telecommunications regulation.

The federal government’s tough anti-spam law, which regulates commercial electronic messages, took effect on July 1, 2014. The law prescribes certain content requirements in electronic messages (such as unsubscribe mechanisms and location information) and restricts sending such messages without appropriate consent. There have been several enforcement actions involving the law. The first CRTC case involved Compu-Finder, a Quebec-based corporate training company that sent commercial emails without consent and without a proper unsubscribe mechanism. Their email practices accounted for a quarter of the complaints in the sector received by the CRTC. In response, the company was hit with a $1.1 million penalty in March 2015.

The CRTC concluded its second case later the same month, this time targeting Plenty of Fish, the popular online dating site. The Commission received complaints that the company was sending commercial emails without a clear and working unsubscribe mechanism. One of the key requirements in the law is that each commercial email contain an unsubscribe mechanism to allow recipients to opt-out at any time. Plenty of Fish agreed to settle the case by paying a $48,000 penalty and developing a compliance program to address its email practices.

Content Removal

With respect to removal of content due to copyright infringement, in 2004 the Supreme Court of Canada ruled that ISPs are not liable for violations committed by their subscribers.\footnote{Society of Composers, Authors & Music Publishers of Canada v Canadian Assn of Internet Providers, [2004] SCC, 2 SCR 427.} Canadian copyright law features a notice-and-notice provision, which, unlike a notice-and-takedown system, does not make intermediaries legally liable for removing content upon notification by the copyright owner. Rather, copyright owners are permitted to send notifications alleging infringement to ISPs. The providers are then required to forward the notifications to the implicated subscriber. Any further legal action is the responsibility of the copyright owner, and it is incumbent upon the person who uploaded the infringing content to remove it following a legal decision. No content is removed from the internet without a court order, and the internet provider does not disclose subscriber information without court approval. ISPs qualify for a legal safe harbor if they comply with the notice-and-notice requirements.

The notice-and-notice requirements took effect on January 2, 2015. Despite the good intentions, the notice-and-notice system has been subject to some misuse. At least one U.S.-based anti-piracy firm, Rightscorp, has used the system to send notifications to subscribers that misstate Canadian law, citing U.S. damage awards and the possibility that their internet access will be terminated, in order to sow fear among Canadians so that they pay a settlement fee.\footnote{Jeremy Malcolm, “Canada Must Fix Rightsholder Abuse of its Copyright Notice System,” Deeplinks Blog, Electronic Frontier Foundation, April 23, 2015, \url{http://bit.ly/1MAANBt}.}

In June 2015, the British Columbia Court of Appeal upheld an earlier decision by the Supreme Court
of British Columbia in *Equustek Solutions Inc. v. Jack*, a closely-watched case involving a court order requiring Google to remove websites that infringed on the plaintiffs’ trademark from its global index. Rather than ordering the company to remove certain links from the search results available through Google.ca, the court’s decision intentionally targeted the entire database, requiring the company to ensure that no one, anywhere in the world, could see the search results. The decision is expected to be appealed to the Supreme Court of Canada.

Defamation claims may also result in the removal of content, as content hosts fear potential liability as a publisher of the defamatory content. Unlike legal protections against liability for copyright infringement by its users, platforms may face liability for alleged defamation once alerted to the publication. A court may also order the removal of the content. A recent Ontario case, *Baglow v. Smith*, involved allegedly defamatory comments posted by a blogger on a political website. Although the Ontario Superior Court decided in favor of the defendants, the court also held that message board operators are not neutral parties to whatever content is exchanged on their platforms. They may, therefore, find themselves liable for defamation if an anonymous individual uses their message board to post a defamatory comment against another individual. Finding otherwise, the court held, would leave plaintiffs without redress when the defamatory comment is made by someone anonymous.  

**Media, Diversity, and Content Manipulation**

The online environment in Canada is relatively diverse, and internet users have access to a wide range of news, content, and opinions. There does not appear to be widespread self-censorship in Canadian online publications, and there is no evidence of government manipulation of online content. Some sites are affiliated with a particular partisan interest, but there are representative sites from all sides of the political spectrum available online. All major media organizations feature extensive websites with articles, audio, and video. The public broadcaster maintains a very comprehensive website that includes news articles and streamed video programming. Paywalls have become increasingly popular among newspaper organizations, but there remains considerable choice (including alternate, independent media) that is freely available.

To date, economic constraints such as net neutrality concerns have not been a significant factor in the success or failure of online media outlets and platforms in Canada, though the debate over net neutrality continues. In January 2015, the CRTC issuing a landmark decision on the net neutrality and “zero-rating” concerns associated with mobile television services offered by Bell and Vidéotron. The CRTC found that, by setting prices that favor their streaming services over others, Bell and Vidéotron had violated the rules that prohibit carriers from granting themselves an undue preference or creating an unreasonable disadvantage for competitors. It noted that the services “may end up inhibiting the introduction and growth of other mobile TV services accessed over the internet, which reduces innovation and consumer choice.” The decision was clearly grounded in net neutrality principles. CRTC Chair Jean-Pierre Blais, speaking prior to the release of the decision, stated that there would be “no fast and slow lanes,” adding that “at its core, this decision isn’t so much about Bell or Vidéotron. It’s about all of us and our ability to access content equally and fairly, in an open market that favors innovation and choice.”

---

13 Baglow v Smith, [2015] ONSC 1175 (CanLII), [http://canlii.ca/t/ggf1t](http://canlii.ca/t/ggf1t).
14 Baglow v Smith.
Digital Activism

Social media and communication applications have been widely used in Canada for the mobilization of political and social movements. The most recent example involved the widespread protests over Bill C-51, the Anti-Terrorism bill, introduced in January 2015. The bill, among other things, introduced criminal penalties for sharing content deemed “terrorist propaganda” or for encouraging others to engage in terrorist acts, and sparked significant online and offline protests, including protests in cities across Canada. Hundreds of thousands of people signed online petitions and raised concerns through digital means. Moreover, the most influential commentary on the bill came through the efforts of Professors Craig Forcese and Kent Roach, who used open access publishing to release hundreds of pages of analysis. The accessibility of Forcese and Roach’s work raised public awareness and ultimately led to several important reforms to the bill.

Violations of User Rights

Despite having a generally positive record for freedom of expression, Canada has taken some regressive steps in recent years, driven by court decisions that weakened confidentiality for journalists’ sources, and the introduction of several bills that could have negative implications for the protection of internet users’ data. Activists have also criticized Conservative Prime Minister Steven Harper’s government for tightening access to information and its slow response time to information requests.

Legal Environment

The Canadian Constitution includes strong protections for freedom of speech and freedom of the press. Freedom of speech in Canada is protected as a “fundamental freedom” by section 2 of the Canadian Charter of Rights and Freedoms. Under the Charter, one’s freedom of expression is “subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.” These laws and protections apply to all forms of speech, whether online or offline.

Hate speech is also regulated under the Canadian criminal code. According to section 320.1, a judge may order that publicly available hate propaganda be made unavailable. In the past, the Canadian Human Rights Commission could investigate and settle complaints regarding online hate speech through section 13 of the Canadian Human Rights Act (CHRA), which prohibits the repeated communication of hate speech over the phone or internet. On June 26, 2013, the parliament passed legislation (Bill C-304) that repealed section 13 of the CHRA, slated to take effect in June 2014. However, in January 2014, a Federal Court of Appeals ruling found section 13 to be constitutionally valid and not a violation of the right to freedom of expression.

There are no specific online restrictions on sensitive topics. Anti-spam legislation, enacted in July 2014, requires opt-in consent to send commercial electronic messages. Critics of the legislation have

---

argued that it is overly broad and seeks to overregulate commercial speech. The constitutionality of the law has not yet been tested.

Defamatory libel is punishable under the criminal code with imprisonment for a term not exceeding five years (s. 301 of the criminal code). Human rights complaints regarding any potentially defamatory statements could also be decided through the mechanisms provided by the Human Rights Code (Ontario) and the Canadian Human Rights Act, in situations where a potentially defamatory statement could also be construed as a violation of the provisions that protect a number of enumerated groups.

Libel tourism, or the practice of taking up a libel case in a jurisdiction considered to be more favorable to the plaintiff, is not a significant problem in Canada, although recent court rulings have called into question whether there are adequate legal protections against such actions. In the case of *Breeden v. Black* in 2012, the Supreme Court issued a ruling confirming that defamation takes place where the content is published; however, as this pertains to the internet, the place where the content is published could mean anywhere the content can be accessed, not just the jurisdiction in which it was uploaded. The court recognized that this interpretation could lead to libel tourism, and indicated a willingness to consider applying the law according to where the most harm was done to the plaintiff’s reputation, which in most cases would be the jurisdiction of their home country.

### Prosecutions and Detentions for Online Activities

Citizens can be subject to legal sanction for possessing, accessing or even distributing child pornography if they post images of it on the internet.18 This also extends to text messages, for example in the January 2014 case of a teenager who sent texts containing explicit images of another teenager and was convicted of possession of child porn.19 Generally, writers, commentators, and bloggers are not subject to legal sanction for content that they post on the internet.

### Surveillance, Privacy, and Anonymity

The past year was a significant one for legislation and court cases involving surveillance and privacy. The Canadian government passed three new laws with privacy implications. In June 2015 the government passed Bill S-4, the Digital Privacy Act, which expanded the scope for companies to make voluntary warrantless disclosures of personal information by allowing for such disclosures to any organization, not just law enforcement. The bill also established new mandatory security breach disclosure requirements and enhanced the meaning of consent within the law.

Bill C-13, the lawful access and cyber-bullying bill, passed in the fall of 2014. The bill created a new warrant that allows a judge to order the disclosure of transmission data where there are reasonable grounds to suspect that an offense has been or will be committed, the identification of a device or person involved in the transmission will assist in an investigation, or will help identify a person. Although this bill preserves judicial oversight of access to metadata, the standard for releasing this data is much lower than the “reasonable grounds to believe” standard, which many thought should

---


have been adopted in the language of the bill. Critics argued that there is reason for concern, as there are significant implications in treating metadata as having a low privacy value. The government passed the bill in the House of Commons in October 2014.

Bill C-51, or the Anti-Terrorism Act, passed in June 2015 also has major privacy implications. The privacy-related concerns stem from Bill C-51’s Security of Canada Information Sharing Act (SCISA), a bill within the bill, which goes far further than allowing for the sharing of information related to terrorist activity. The bill permits information-sharing across government for an incredibly wide range of purposes, most of which have nothing to do with terrorism. The government tried to justify the provisions on the grounds that Canadians would support sharing information for national security purposes, but the bill allows sharing for reasons that would surprise and disturb most Canadians. The bill was opposed by all Canadian privacy commissioners, but ultimately passed and became law.

Privacy was also a major issue in the courts and in complaints to the privacy commissioner of Canada. The most notable case was the Supreme Court of Canada’s R. v. Spencer decision, released in June 2014.20 The Spencer decision, which examined the legality of voluntary warrantless disclosure of basic subscriber information to law enforcement, called into question longstanding practices and forced law enforcement and other agencies to re-examine their approach. In a unanimous decision written by Justice Thomas Cromwell, the court issued a strong endorsement of internet privacy, emphasizing the privacy importance of subscriber information, the right to anonymity, and the need for police to obtain a warrant for subscriber information except in exigent circumstances or under a reasonable law. This ruling also calls into question the legality of several privacy-related bills passed during the coverage period.

In December 2014, the Supreme Court of Canada issued its decision in R. v. Fearon, a case involving the legality of a warrantless cellphone search by police during an arrest. To the surprise of many, a divided court upheld the ability of police to search cellphones without a warrant incident to an arrest. The majority opinion established some limiting conditions, but ultimately ruled that it was possible navigate the privacy balance by establishing some safeguards with the practice. A strongly worded dissent noted the privacy implications inherent in warrantless access to cellphones and the need for judicial pre-authorization as the best method of addressing these implications.

The Office of the Privacy Commissioner provides an important oversight function related to privacy of Canadians’ information in the digital medium. The Privacy Commissioner of Canada is an officer of parliament who reports directly to the House of Commons and the Senate. Daniel Therrien was appointed Privacy Commissioner of Canada beginning June 5, 2014. The commissioner’s mandate includes overseeing compliance with the Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, and the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada’s private sector privacy law.21 In March 2015, the Privacy Commissioner of Canada issued an important finding on the legality of online behavioral advertising, ruling that a targeted advertising program run by Bell violated the law.

**Intimidation and Violence**

There were no documented cases of violence or physical harassment of internet users in Canada for their online activities during the report period.

---

Technical Attacks

There have been several high profile cyberattacks and data breaches in Canada, including some that have involved the government. In July 2014, the Canadian government blamed Chinese hackers for a cyberattack on the Canadian National Research Council. Subsequently, in June 2015, another cyberattack crashed several government websites and e-mail services. The international group Anonymous claimed responsibility for this attack, citing it as a protest against the passage of the Bill C-51 Anti-terrorism Act.22

China

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Free</td>
<td>Not Free</td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>19</td>
<td>18</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>39</td>
<td>40</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>87</td>
<td>88</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 1.36 billion
Internet Penetration 2014: 49 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2015 Status: Not Free

Key Developments: June 2014 – May 2015

- In January 2015, Chinese authorities reported an upgrade to the national firewall that blocked several providers of virtual private networks in the name of “cyberspace sovereignty” (see Blocking and Filtering).
- The China Internet Network Information Center was found to be issuing false digital security certificates for a number of websites, including Google, exposing the sites’ users to “man in the middle” attacks (see Technical Attacks).
- The government strengthened its real-name registration laws for blogs, instant-messaging services, discussion forums, and comment sections of websites (see Surveillance, Privacy, and Anonymity).
- In November 2014, the Chinese government introduced a draft counterterrorism law that would require all telecommunications companies and internet services to provide the government with “backdoor” access and copies of encryption keys (see Surveillance, Privacy, and Anonymity).
Introduction

The Chinese Communist Party (CCP) under general secretary and state president Xi Jinping continued to pursue “cyberspace sovereignty” as a top policy strategy during the coverage period of this report. The aim of establishing control was particularly evident in the government’s attitude toward foreign internet companies, its undermining of digital security protocols, and its ongoing erosion of user rights, including through extralegal detentions and the imposition of prison sentences for online speech. China was the world’s worst abuser of internet freedom in the 2015 Freedom on the Net survey.

The groundwork for this intensifying strategy of control was laid during the previous coverage period. In an internal speech at the National Propaganda and Ideology Work Conference in August 2013—first publicized by military and party commentators, and later revealed in full by China Digital Times—Xi declared that “the internet has become the main battlefield for public opinion struggle.” This represented considerably stronger rhetoric than that used by his predecessor, Hu Jintao, who had merely referred to “guidance” and “channeling” of public opinion online. The new terminology provided the ideological underpinning for the internet freedom decline that has continued since. Lu Wei, head of the State Internet Information Office (SIIO), articulated his approach in concrete terms, proposing more licensing for online platforms, more real-name registration, more information-management training for government and private-sector agents, and tighter controls on undesirable content. Lu Wei appears increasingly central to Xi’s internet strategy, and was appointed in February 2014 to a panel on information technology and security policy that the president himself has chosen to lead, assuming a role usually played by the premier. This high-level committee positioned internet development, governance, and security as high-priority issues for Xi’s administration, along with national security and economic reform.

Over the past year, the renewed emphasis on information control led to acts of unconcealed aggression against internet freedom. All of Google’s content and communication services were fully blocked during the coverage period, marking an escalation in censorship from that experienced by the company’s user base in mainland China in previous years. A government agency was found to be issuing false digital security certificates for a number of websites, including Google, leaving visitors to those sites vulnerable to attacks from hackers who replace webpages with unverified facsimiles in order to deliver malware or steal personal data. And the University of Toronto–based research group Citizen Lab documented massive cyberattacks on U.S. anticensorship websites that originated in the architecture of the Chinese government’s own censorship apparatus, known as the Great Firewall—a previously undocumented capability that the group dubbed the Great Cannon.

As in past years, although pressure on overseas websites and companies increased, the real targets of repression were domestic internet users. Individuals imprisoned for legitimate online speech during the coverage period included renowned human rights lawyer Pu Zhiqiang, who was criminally

---

3 “State Internet Information Office Director Lu Wei outlines stronger focus on Internet governance,” China Copyright and Media (blog), September 17, 2013, [http://bit.ly/1JhwP0D](http://bit.ly/1JhwP0D).
China

charged with inciting ethnic hatred and picking quarrels on social media, and 70-year-old journalist Gao Yu, who was jailed for seven years for supposedly leaking “state secrets” to an overseas website.

There were some examples of public activism, reflecting the vibrancy that is still common on the Chinese internet. An online petition in support of five feminists who were detained for distributing leaflets against sexual harassment on public transportation may have contributed to their release in April 2015.\(^6\) And the environmental documentary *Under the Dome* was viewed by millions of people online before it was censored. But despite these efforts, and steady improvements in access year on year, internet control is intensifying.

**Obstacles to Access**

*China boasts the world’s largest number of internet users, yet obstacles to access remain, including poor infrastructure, particularly in rural areas; a telecommunications industry dominated by state-owned enterprises; centralized control over international gateways; and sporadic, localized shutdowns of internet service to quell social unrest. Nationwide blocking, filtering, and monitoring systems delay or interrupt access to international websites.*

**Availability and Ease of Access**

The authorities reported in January 2015 that there were 649 million internet users in China.\(^7\) The average connection speed was comparatively slow at 3.8 Mbps.\(^8\) Since 2011, internet adoption rates have slowed as the urban market approaches saturation, according to the China Internet Network Information Center (CNNIC), an administrative agency under the Ministry of Industry and Information Technology (MIIT).\(^9\) Though the digital divide between urban and rural areas narrowed marginally in 2014, 72.5 percent of users were based in cities, and more were documented in Eastern China than in the less developed Central and Western regions combined.\(^10\) Penetration rates vary by province, from Beijing (75 percent) to Jiangxi in the southeast (32 percent).\(^11\) Overall internet penetration stood at 48 percent.\(^12\) The CNNIC continued to report a gender gap among internet users, with males making up 56 percent of the total.

Mobile replaced fixed-line broadband (which had dwarfed dial-up since 2005\(^13\)) as China’s preferred means of accessing the internet for the first time in 2012. From December 2013 to December 2014,

---

11. CNNIC, 中国互联网络发展状况统计报告.
12. CNNIC, 中国互联网络发展状况统计报告.
the mobile internet population grew from 500 million to 557 million, accounting for 86 percent of all internet users.14 Authorities exercise tight control over cybercafes and other public access points, which are licensed by the Ministry of Culture in cooperation with other state entities.15 By 2012, chain companies had absorbed around 40 percent of cybercafes.16 Domestic news reports said more than 10,000 locations closed between 2011 and 2012, and cybercafes provided access for less than 20 percent of internet users in 2013.17 In November 2014, the Chinese government reversed its policy and loosened restrictions on opening up cybercafes, lifting a 2013 requirement that they had to be run by chain stores, which had led to the proliferation of illegal establishments.18 Though demand remained relatively high in rural areas and small towns, the number of internet users throughout China who were connecting through cybercafes and public computers remained relatively constant in 2014, at 18 percent.19

Costly, inefficient fixed-line broadband service has contributed to the shift toward mobile. The Beijing-based research company Data Centre of China Internet reported that the average cost of 1 Mbps of bandwidth was 469 times more on the mainland than in Hong Kong in 2011.20 The MIIT ordered that homes constructed within reach of public fiber-optic networks be connected via a selection of service providers from April 2013 onward.21 A “Broadband China” government strategy issued in August 2013 aimed to boost penetration to 70 percent nationwide by 2020, raise third-generation (3G) mobile internet penetration to 85 percent, and increase connection speeds to 50 Mbps in cities and 12 Mbps in rural areas, with even faster Gbps speeds promised in bigger cities.22 By the end of 2014, however, the average fixed-line broadband download speed across the country was still only 4.25 Mbps. The highest available rate was in Shanghai, which averaged 5.3 Mbps, while the lowest was in Tibet, which averaged 3.26 Mbps.23

Restrictions on Connectivity

Nine state-run operators maintain China’s gateways to the global internet, giving authorities the ability to cut off cross-border information requests.24 All service providers must subscribe via the gateway operators under MIIT oversight.

---

23 Broadband and Development Alliance, China’s broadband speed status report [in Mandarin], Section 6, http://bit.ly/1NbmZfX
China

The government has shut down access to entire communications systems in response to specific events, notably imposing a 10-month internet blackout in the Xinjiang Uyghur Autonomous Region—home to 22 million people—after ethnic violence in the regional capital, Urumqi, in 2009. Since then, authorities have enforced smaller-scale shutdowns, including one in September 2014 in Xinjiang’s Yarkand (known in Chinese as Shache) County that began during the month of Ramadan and affected internet access and text-message services amid increasing tension between the Uyghur ethnic minority and the Chinese government.

ICT Market

In 2011, an antimonopoly investigation accused state-owned China Telecom and China Unicom of abusing their market dominance to manipulate fixed-line broadband pricing, marking the first use of a 2008 antimonopoly law against state enterprises. The telecom giants revised their inter-network pricing structures to allow rivals to access their infrastructure, and customers can now choose from among 20 local, private internet service providers (ISPs), but these only account for 10 percent of the market share.

State-owned China Mobile, China Telecom, and China Unicom dominate the mobile market, but other companies can provide telecommunications service by leasing network infrastructure. High prices have slowed 3G adoption in China, especially as some social-networking platforms allow users to exchange messages at low cost via 2G handsets, which accounted for 31 percent of mobile internet access in 2013, according to one report. In May 2014, the government formally authorized the three major players to set pricing for services according to market forces, resulting in price cuts. On February 27, 2015, the MIIT reported that it had issued licenses to China Telecom and China Unicom to operate 4G wireless networks.

Regulatory Bodies

Several government and CCP agencies are responsible for internet censorship at the local and national levels, but the process has been consolidated under Xi Jinping. The SIIO was created in 2011 to streamline regulation of online content, punish violators, and oversee telecommunications

32 Gerry Shih, “China issues 4G FDD licenses to China Telecom, China Unicom,” Reuters, February 27, 2015, http://reut.rs/1NFav6Q.
companies. Initially under the State Council Information Office, the agency was streamlined and rebranded during the coverage period of this report. On August 26, 2014, the State Council formally authorized the SIIO to regulate and supervise internet content. In December 2014, it launched a new website under the English translation Cyberspace Administration of China (CAC), and with a new organizational affiliation to the Office of the Central Leading Group for Cyberspace Affairs. That office, also known by the English name Central Internet Security and Informatization Leading Group, was formed in February 2014, directly under Xi, to oversee cybersecurity, making it highest authority on internet policy in China. In December 2014, the leading group took charge of the CNNIC, which issues digital certificates to websites.

Two regulatory bodies, the State Administration of Radio, Film, and Television (SARFT) and the General Administration for Press and Publications (GAPP), both responsible for censorship in their respective sectors, merged in 2013 to form the State Administration of Press, Publications, Radio, Film, and Television (SAPPRFT). The new regulatory body’s tasks include monitoring internet-based television and online videos.

**Limits on Content**

The CCP propaganda department, government agencies, and private companies employ thousands of people to monitor, censor, and manipulate content. A range of issues are systematically censored, including independent evaluations of China’s human rights record, critiques of government policy, and the authorities’ treatment of ethnic minorities. Routine censorship is reinforced during politically sensitive events or in response to breaking news. However, even this heavily manipulated online environment provides more space for average citizens to express themselves or criticize the state than any other medium in China.

**Blocking and Filtering**

The Chinese government uses a sophisticated and ever-evolving censorship apparatus, incorporating both automated mechanisms and human monitors, to block and filter material that criticizes or challenges individuals, policies, or events considered integral to the one-party system. Politically sensitive events that drew censorship during the coverage period included the 25th anniversary of the Tiananmen Square crackdown and Hong Kong’s prodemocracy “Occupy Central” protests, also known as the Umbrella Revolution.

Over the last several years, censors have increasingly blocked international news websites for their reporting on corruption and illicit wealth among high-level officials, as well as a range of other issues thought to challenge the government. Foreign-based news organizations with Chinese-lan-
guage websites are a particular target. As of March 24, 2015, at least 14 of 18 news websites tracked by the nonprofit news organization ProPublica were inaccessible inside China. The system responsible for such automated, technical blocking of foreign websites is commonly referred to as China’s “Great Firewall.” In some cases, whole domain names or internet protocol (IP) addresses are blocked, with users receiving an explicit message about illegal content. Other interventions are less visible. For example, observers have documented unusually slow speeds that indicate deliberate throttling, which delays the loading of targeted sites and services.

Authorities also use deep packet inspection (DPI) to scan both a user’s request for content and the results returned for any blacklisted keywords. Once these are detected, the technology signals both sides of the exchange to temporarily sever the connection. Such granular control is less noticeable to users because specific pages can be blocked within otherwise approved sites, and because the interruption appears to result from a technical error. Returning fake pages, or replacing the requested site with content retrieved from an unrelated IP address using a technique known as DNS poisoning, is another routine method of disrupting access to specific content. During the coverage period, websites hosting content and services that were not explicitly banned still found themselves temporarily offline because their web address had been substituted for another on the blacklist, overwhelming them with requests from Chinese users; in at least one reported case, a search for banned censorship-circumvention software was redirected to pornographic content.

In practice, filtering varies depending on timing, technology, and geographical region. ISPs reportedly install filtering devices differently, in the internet backbone or even in provincial-level internal networks, a development that would potentially allow interprovincial filtering. The University of Macau’s new campus in southern Guangdong Province has advertised unfiltered internet access, but there were no reports during the coverage period on whether this had actually taken effect. As students led political protests in Taiwan and Hong Kong in 2014, censors sought to shut off their online interaction with the mainland, disrupting mainland access to chat applications that were used to organize the demonstrations, like KakaoTalk and LINE, and censoring vocabulary specific to the ongoing political developments.

Software developers, both domestic and overseas, have created applications offering access to virtual private networks (VPNs), which encrypt the user’s traffic and reroute it through a server outside the firewall to circumvent technical filtering. As of November 2014, China boasted the largest number of VPN users in the world, nearly 93 million, according to GlobalWebIndex.

---

46 Jason Mander, “90 Million VPN users in China have accessed restricted social networks,” GlobalWebIndex blog, November
In January 2015, Chinese authorities reported an upgrade to its national firewall that blocked several providers of VPNs, including Astrill (based in Seychelles), StrongVPN (based in the United States) and Golden Frog (registered in Switzerland). Officials claimed that the upgrade was meant to uphold “cyberspace sovereignty.” Even when not actively disrupted, encrypted internet activity may attract surveillance.

Certain internationally popular web applications are totally blocked, isolating the Chinese public from a global network of user-generated content. According to GreatFire.org, an organization that monitors blocked content in China, 169 of Alexa’s top 1,000 websites in the world were blocked in 2014, up from 62 the year before. These include Google, Facebook, Flickr, SoundCloud, and WordPress.

In May 2015, five days before the 25th anniversary of the Tiananmen Square crackdown, Google’s remaining services were fully blocked, including Google Maps, Translate, Calendar, and Scholar, and they remained so as of May 2015. Google Analytics, which provides audience data to website owners, remained operational, according to the London-based Guardian newspaper. Other social media services like the photo-sharing platform Instagram and Viber were blocked during the Umbrella Revolution protests that shook Hong Kong in the autumn of 2014.

In July 2014, Instagram was removed from online Android application stores run by the Chinese services Baidu, Xiaomi, Wandonjia, Qihou360, Tencent, and 91 Wireless. Users who had previously downloaded the Instagram app were still able to use it, but not if they were on China Mobile’s 3G network, which had never allowed access to Instagram’s servers.

Many social media applications produce sanitized versions for the mainland Chinese market. In 2012, Evernote launched a separate service for the Chinese mainland, with modified terms of use containing a list of nine categories of “undesirable information.” In January 2015, it disabled the public note feature, which had been used to share news and information about Hong Kong’s Umbrella Revolution.

LinkedIn, which censors briefly blocked in 2011, launched a Chinese-language version in early 2014. “We are opposed to censorship … [but] that’s going to be necessary for us to achieve the kind of scale that we’d like to be able to deliver to our membership,” Chief Executive Jeff Weiner told the Wall Street Journal. LinkedIn informed users when their content would not be visible in China.

Search requests that include blacklisted keywords also trigger China’s censorship apparatus, produc-
China

In 2014, censorship intensified in advance of the 25th anniversary of the crackdown on student-led protests to encompass phrases like “return to Tiananmen,” “89,” ”8 squared,” and “Victoria Park,” the Hong Kong site of a massive annual vigil. In May, one blog reported that a user-generated encyclopedia hosted by Baidu had entries for the years 1988 and 1990, but not 1989.

Even the names of prominent activists are often censored. Examples during the coverage period include “Pu Zhiqiang,” after the renowned human rights lawyer was detained in Beijing in May 2014, and “Ilham Tohti,” the Uyghur scholar who was sentenced to life in prison on “separatism” charges for his essays defending Uyghur rights online.

The censorship backlash against forums on “constitutionalism” continued during the coverage period. Discussion of the concept was banned on at least one platform in 2014 after it became associated with a fledgling civic movement, suggesting that social movements are perceived as more of a threat than opinions or discussions on their own. According to one 2014 study, “even posts that praise the government are censored if they pertain to real-world collective action.”

Content Removal

In the past, the government has not been transparent about content controls, telling international reporters in September 2013 that “the perception that the government has placed any restrictions on the internet is untrue.” However, a draft cybersecurity law, released to the public outside the coverage period in July 2015, makes it clear that the authorities are tasked with imposing such restrictions. The legislation states that the “national cyberspace administration and relevant departments perform network security supervision and administration responsibilities; and where discovering information the release or transmission of which is prohibited by laws [or] administrative regulations, shall request the network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside mainland People’s Republic of China, they shall notify the relevant organization to adopt technological and other necessary measures to block the transmission of information.”

Still, censorship decisions are arbitrary, opaque, and inconsistent, in part because so many individuals and processes are involved. Blacklists periodically leak online, but they are not officially published. There are no formal avenues for appeal. Criticism of censorship is itself censored.67

Antipornography and antirumor campaigns are a long-standing cover for censorship of social and political content. On January 19, 2015, the SIIO announced the shutdown of 133 public accounts on the social media site Weixin—whose international version is known as WeChat—that had purportedly spread false information about the history of the CCP and the country.68 On March 25, the SIIO published new guidelines outlining prohibited content on Weixin, specifically targeting sexually explicit material, but also banning stories of “one-night stands, wife-swapping, sexual abuse and other harmful information,” according to Reuters.69

Mobile service providers monitor text messages and delete pornographic or other “illegal” content.70 Users report receiving blank messages in place of banned keywords, though what content is banned appears to vary.71

Instant-messaging services such as TOM-Skype and QQ include programming that downloads updated keyword blacklists regularly.72 Other companies employ human censors to delete posts, sometimes before they appear to the public.73 Experts say staff members receive as many as three censorship directives per day by text message, instant message, phone call, or e-mail.74 Most come from local propaganda officials. However, the CCP established party branches within four microblog company offices in 2012 to improve compliance, according to news reports.75 In a November 2013 article published in Tibet, the local party leader pledged to establish CCP units or send political instructors to conduct ideological education in website offices.76

Provincial police also have authority to issue takedown notices to local companies. In April 2014, local and international media reported that Wei Yining, an internet police official in Hainan Province, had recently been sentenced to 10 years in prison for accepting more than 280 bribes to issue such notices to Hainan-based web forums Tianya and Kaidi. The bribes were paid by internet police in other jurisdictions, who should have submitted their deletion requests to Wei’s department for approval, but instead paid him to contact the companies directly via instant message. One colleague in Hubei Province paid 483,000 yuan (US$78,000) in one year.77

68 CAC, “SIIO: 133 public accounts that disseminate false information about the history of the Party and country had been closed down according to the law,” http://www.cac.gov.cn/2015-01/19/c_11140517959.htm.
73 King, Pan, and Roberts, “How Censorship in China Allows Government Criticism but Silences Collective Expression.”
77 Josh Chin and Yang Jie, “Corruption Case Cracks Door on China’s Internet Police,” China Real Time, Wall Street Journal, April 18, 2014, http://on.wsj.com/1fLq2Cmv; “More Details Emerge of Internet Police Involved in Nationwide Money-For-
Other content has been suppressed by private actors. In June 2014, Beijing-based Caixin magazine reported that a China Central Television (CCTV) executive under investigation for bribery had asked website operators to delete posts on behalf of other companies. Search engines also remove or highlight results, possibly squelching negative items about their own performance, according to one analysis.

In March 2015, Under the Dome, a critically acclaimed documentary detailing China’s air pollution that was viewed by over 150 million users on Tencent alone and praised by the environment minister, was pulled from domestic video-sharing websites after it gained widespread attention.

Media, Diversity, and Content Manipulation

Online journalists regularly practice self-censorship. Editors and reporters who post banned content, or content that is critical of the CCP, its high-ranking members, or its actions, now or in the past, risk disciplinary warnings, job loss, or even criminal detention. Authorities warned online news providers of tighter scrutiny in 2015, and threatened the web portal Sina with suspension in April for failing to prevent violations. In May, the agency published a list of news organizations that were “authorized to provide websites for reposting news.”

Propaganda officials also manipulate online content, instructing internet-based outlets to amplify content from state media. In one example from the coverage period, the State Council Information Office reportedly issued this directive: ‘All media must refrain from further promoting [the environmental documentary] ‘Under the Dome.’ Online public opinion [surrounding the documentary] must be regulated.”

Since 2005, propaganda units at all levels have trained and hired web commentators, known colloquially as the “50 Cent Party,” to post progovernment remarks and influence online discussions. These commentators also report users who have posted offending statements, target government critics with negative remarks, or deliberately muddy the facts of a particular incident. Coordinated smear campaigns are used to discredit high-profile government critics.

A document leaked in January 2015 revealed that there are 350,000 “Youth League Online Censorship Scheme.”

---

79 “Caixin Report Provides Context for Baidu's 2011 Censorship.”
86 These propaganda workers are colloquially known as the 50 Cent Party due to the amount they are reportedly paid per post, though recent reports put the going rate as low as 10 cents, while some commentators may be salaried employees. See Perry Link, “Censoring the News Before It Happens,” New York Review (blog), New York Review of Books, July 10, 2013, http://bit.ly/1b1v7Tt.
mentators” in China’s higher-education institutions, tasked with swaying students against supposed Western values. The work also extends beyond China’s borders to social media apps that are actually banned for mainland users, such as Twitter. Approximately 2,500 “50 Cent” users on Twitter follow and retweet one another in order to create confusion and mislead the public. In July 2014, it was revealed by the London-based organization Free Tibet that propagandists had opened scores of fake accounts on Twitter to glorify China’s Tibet policies. Other such fake accounts were created in an attempt to smear dissidents, notably the writer Hao Qun, known by his pen name Murong Xuecun, who wields considerable influence online both domestically and internationally, but whose Sina Weibo microblogging account was deleted in a 2013 purge.

These methods are not always effective, however. Many government-paid commenters are more concerned about filling their quota than mounting a convincing argument, and web users are wary of content manipulation. Companies also pay for “astroturfing”—positive comments promoting products or services—which further erodes public trust in online content. (Commercial commenters are colloquially known as the “internet water army.”) However, in January 2015 the SIIO, MIIT, Ministry of Public Security, and SAPPRFT launched a joint campaign against “internet blackmail and paid content removal,” cracking down on companies that accept fees for deleting “unfavorable” posts.

In March 2014, the state news agency Xinhua announced the latest round of internet supervision training courses for officials across government institutions, including the police and the judiciary. The courses, which offer five qualifications from assistant to senior manager, cost 6,800 yuan (US$1,108). Government employees also openly engage citizens in online discussions. In October 2013, an opinion-monitoring official at the People’s Daily newspaper, an official CCP mouthpiece, said that the quantity of posts by the Weibo accounts of traditional media outlets and government officials or entities had overtaken the output of high-profile online opinion leaders with mass followings, known as Big Vs.

Nationalism and xenophobia are prominent components of Chinese cyberspace, though censorship that targets rational dissent instead of inflammatory discourse arguably magnifies their impact. In March 2014, when students in Taiwan occupied the legislature to protest against a free-trade pact with China, Weibo said 60 percent of microbloggers polled called the action “irrational,” but the service censored posts that compared the incident to China’s 1989 student protests.

---

92 Xuecun, “Beijing’s Rising Smear Power.”
Still, political discourse can be vigorous online, even about democracy and constitutional government. This is partly because the leadership redefined democratic governance as “the Chinese Communist Party governing on behalf of the people” in 2005. A certain amount of open discussion also allows officials to monitor public sentiment, debunk “enemy” ideology without triggering censorship, and conduct internal power struggles. Censors employed by Sina allowed “more room for discussions on democracy and constitutionalism because there are leaders who want to keep the debate going,” according to one report.

Domestic internet firms benefit commercially from the blocking of foreign social media, but they are obliged to prevent banned content from circulating as part of their licensing requirements. Chinese company executives also enjoy political patronage.

More than half of China’s internet users had registered for a microblog account by January 2013. Many companies offer services, but the most prominent are Sina Weibo and Tencent’s Weixin. In April 2013, news agencies were told to register official microblog accounts with their government sponsor.

Weibo’s distinct feature is the comment thread developed in response to individual posts; the threads are lost if the original post is censored, and the feature can also be shut off to prevent a given post from gaining traction. In March 2014, Sina’s prospectus to the U.S. Securities and Exchange Commission reported 129 million Weibo users active every month and 61 million active daily, though a research study from Hong Kong said the majority of posts were generated by just 10 percent of users, while thousands of others were zombie accounts created for marketing purposes. Sina’s efforts to manage Weibo content are well documented. Staff, reportedly 150 people working 12-hour shifts, delete individual posts or accounts, often within 24 hours of an offending post, but sometimes long after publication; make published posts visible only to the account owner; and personally warn individual users.

110 Xiao, “From ‘Grass-Mud Horse’ to ‘Citizen’: A New Generation Emerges through China’s Social Media Space.”
China

Weibo was punished with restrictions on some of its functions in 2012 for failing to curb “rumors.” In 2013, following an intensified antirumor campaign, Weibo said 1,000 accounts had been shuttered for posting false information, out of a total 100,000 accounts that were disabled for harassment and other violations. Activity on the platform dropped by an estimated 70 percent. In January 2014, the CNNIC reported that 38 percent of Weibo users had migrated to Weixin.

In 2015, Tencent reported a combined 500 million monthly active users for Weixin and its international equivalent. Some activists prefer Weixin because users have the option to restrict updates to a closed circle of connections, and can send audio messages that bypass keyword censorship. Yet the service still monitors and restricts political content. In what users described as a “massacre” in March 2014, just before the coverage period, Weixin closed dozens of accounts, including one run by investigative journalist Luo Changping.

Despite the technical filtering, enforced self-censorship, and manipulation, the internet is a primary source of news and forum for discussion, particularly among the younger generation. Chinese cyberspace is replete with online auctions, social networks, homemade music videos, a large gaming population, and spirited discussion of some social and political issues. Overtly political organizations, ethnic minorities, and persecuted religious groups remain underrepresented, though they have used the internet to disseminate banned content, and overseas media and human rights groups report sending email to subscribers in China with news, instructions on circumvention technology, or copies of banned publications. Civil society organizations involved in charity, education, health care, and other social and cultural issues often have a vigorous online presence.

Users combat censorship by opening versions of the same blog on different sites and circulating banned information directly through peer-to-peer networks, which bypass central servers. Text rendered as image, audio, or video files evades keyword sensors. Humorous neologisms, homonyms, and cryptic allusions substitute for banned keywords, forcing censors to filter seemingly innocuous vocabulary like “tiger.” This version of the Chinese internet does not resemble a repressed information environment so much as “a quasi-public space where the CCP’s dominance is being constantly exposed, ridiculed, and criticized, often in the form of political satire, jokes, videos, songs, popular poetry, jingles, fiction, Sci-Fi, code words, mockery, and euphemisms.”

[121] Xiao, “From ‘Grass-Mud Horse’ to ‘Citizen’: A New Generation Emerges through China’s Social Media Space.”
China

Digital Activism

The word “netizen”—a direct translation of the Chinese wangmin, or citizen of the internet—conveys the legitimate sense of civic engagement associated with online exchanges. Microblogs have amplified these dynamics and generated a strong sense of empowerment among many Chinese users, censorship notwithstanding.122 Whereas Chinese citizens traditionally trek to the seat of power to present their grievances, digital technologies offer a way to overcome the geographic, financial, and physical challenges of such petitioning. Moreover, despite the leadership’s dread of collective action, officials do yield to public pressure. Low-level government wrongdoing, once exposed by users, is often punished, with officials frequently singled out for overspending on entertainment or designer watches, a sign of possible corruption.123 Officials do seek to gauge, and are influenced by, the public mood.

The transformative effect of online activism in China is undeniable, and yet the final outcomes of high-pressure encounters between netizens and officials typically fall short of systemic reform or democratic decision-making. Consequently, they fail to ensure meaningful accountability.124 Censors intervene if campaigns gain too high a profile or implicate overall CCP governance. In the past year, some nongovernmental organizations found their ability to fundraise using e-commerce platforms obstructed, including a rural library project that was forced to close in September 2014.125

In April 2015, a campaign to release five feminists who had been detained in March for distributing leaflets against sexual harassment on public transportation gained momentum, with an online petition signed by over 1,000 people that had circulated via private email and encrypted social-media messaging systems.126 The women were released on April 13, but they remained under surveillance.

Violations of User Rights

A number of criminal laws and internet regulations ensnare users who post content deemed undesirable by the CCP. Authorities use antipornography and antirumor campaigns as a cover for suppressing politically sensitive material and voices, and charges typically used to silence offline dissent—subversion, separatism, and terrorism, as well as defamation and “creating a disturbance”—are regularly invoked to imprison citizens for their online activity. A bolstered “real-name registration” system remains a threat to users’ privacy and anonymity, and surveillance has increased in ethnic minority areas chafing under CCP rule. Websites, hosting services, and dissidents’ email accounts are routinely attacked by hackers based in China.

124 According to one study, censors stopped blocking naming of villages whose residents were protesting as soon as traditional media reported on the provincial authorities’ response, even though tensions had not yet fully died down and the effectiveness of the response had yet to be shown. In other words, reports on protests in the context of an ostensibly benevolent response from party officials are not censored. See Freedom House, “Finnish Study Analyzes Keyword Censorship during Mass Incidents,” China Media Bulletin, December 13, 2012, http://www.freedomhouse.org/cmb/77.121312t5.
China

Legal Environment

Article 35 of the Chinese constitution guarantees freedoms of speech, assembly, association, and publication, but such rights are subordinated to the CCP's status as the ruling power. In addition, the constitution cannot, in most cases, be invoked in courts as a legal basis for asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive freedom of expression cases. China lacks specific press or internet laws, but government agencies issue regulations to establish censorship guidelines. Regulations—which can be highly secretive—are subject to constant change and cannot be challenged by the courts. Prosecutors exploit vague provisions in China's criminal code; laws governing printing and publications; subversion, separatism, and antiterrorism laws; and state secrets legislation to imprison citizens for online activity.

The legal grounds for these charges were strengthened in 2013. In September, the Supreme People's Court and the Supreme People's Procuratorate, the top prosecutorial body, issued a judicial interpretation entitled “Regarding the Interpretation of Various Laws Concerning the Handling of Cases of Using the Internet to Carry Out Defamation and Other Crimes,” which formally defined online manifestations of crimes including defamation, creating disturbances, illegal commercial activities, and extortion.127 Local officials had already detained online whistle-blowers for criminal defamation, which carries a possible prison term of three years under “serious” circumstances.128 But the new interpretation defined those circumstances to cover defamatory online content that receives more than 5,000 views or is reposted more than 500 times.129 Online messages deemed to incite unrest or protest are also subject to criminal penalties under the interpretation.

Bloggers and activists periodically use the law to defend their right to online expression. In July 2014, Wang Long,130 a resident of Shenzhen, Guangdong Province, sued China Unicom for failing to provide access to Google services during the block that began in May 2014. A local court in Shenzhen’s Futian district heard the case, the first of its kind, in September 2014.131 Though many legal challenges lack the resources or the political backing to succeed, in April 2014, a court in Guangdong ordered the local health and family planning commission to reprocess a 2007 request submitted under open-government regulations. The commission had declined to release records about resource allocation to a lawyer based in Zhejiang, who successfully sued for it to reconsider.132
Prosecutions and Detentions for Online Activities

Reporters Without Borders documented a total of 84 netizens in Chinese jails as of September 2015.\(^{133}\)

Netizens and activists have been detained in a series of crackdowns over the last several years that were aimed at curtailing protests and perceived threats to “social and public order.” Those affected have included lawyers who utilized social media to advocate for civil society, like Xu Zhiyong, and well-known online commentators and bloggers who were accused of “spreading rumors online.”

On April 24, 2014, authorities detained renowned 70-year-old journalist Gao Yu, a contributor to the German news outlet Deutsche Welle, for “leaking state secrets.” Official media alleged that Gao provided a secret document of the CCP Central Committee (believed to be Document No. 9, which warned officials to be vigilant about “seven subversive elements” in society, including human rights) to a foreign website, which published it in full. Her closed-door trial took place on November 21, 2014, but a verdict was not handed down until April 17, 2015, when Gao was convicted and sentenced to seven years in prison.

Pu Zhiqiang, a human rights lawyer, was detained in Beijing on May 6, 2014, on suspicion of “picking quarrels” after he attended a May 3 seminar about the 25th anniversary of the Tiananmen Square crackdown. He was formally arrested on June 13. Pu has been charged with creating a disturbance, inciting ethnic hatred, and separatism, based on 28 posts Pu made on Weibo between July 2012 and May 2014—the prosecution’s only evidence.\(^{134}\) In May 2015, a year after his detention, the procuratorate announced that Pu would stand trial for inciting ethnic hatred and picking quarrels.\(^{135}\) A trial date was not immediately released.

The Hong Kong prodemocracy protests of September and October 2014 triggered another wave of arrests. Nearly two dozen people were detained for expressing support for the growing protests. Wang Long, the rights advocate in Shenzhen who had filed a lawsuit against China Unicom for censoring Google earlier in 2014, was detained on September 27, 2014, on charges of “creating a disturbance” after he forwarded news reports about the protests.\(^{136}\)

Hundreds were detained in the ongoing campaign to crack down on alleged online rumor-mongering, and in August 2014 state authorities announced that they had arrested four people and detained another 81.\(^{137}\) Dong Rubin, a Yunnan-based blogger with 50,000 followers who is known for his criticism of party officials, police brutality, and environmental hazards, was sentenced to six and a half years in prison in July 2014.\(^{138}\)


\(^{134}\) Chris Buckley, “Comments Used in Case Against Pu Zhiqiang Spread Online,” Sinosphere (blog), New York Times, January 29, 2015, \url{http://nyti.ms/1GGuHNN}.


\(^{136}\) Andrew Jacobs, “Detentions of Hong Kong Protest Sympathizers Reported in Mainland,” October 1, 2014, New York Times, \url{http://nyti.ms/1R9z2F}.

\(^{137}\) “85 people ‘arrested or detained’ as China steps up clampdown on internet rumours,” South China Morning Post, August 9, 2014, \url{http://bit.ly/1Hd6X84}.

China

As in past years, religious and ethnic minorities faced particularly harsh treatment for online activity. In July 2014, a 22-year-old Uyghur man was detained for “rumor-mongering” following violent clashes in Xinjiang’s Yarkand (Shache) County; he had alleged in an online post that Chinese security forces killed thousands of people. The man, a resident of Urumqi who was not publicly identified, uploaded the article onto an overseas website.139 Internet service was shut down in Yarkand, and international observers were denied access to the area.

In January 2014, professor, writer, and Uyghur rights advocate Ilham Tohti was detained in a raid on his Beijing home. He was later indicted for allegedly spreading rumors, inciting ethnic hatred, and conducting separatist activities on a website he founded.140 Separatism charges carry a possible death penalty in extreme cases. In September 2014, a court sentenced Tohti to life imprisonment.141 Seven of his students, who had helped him with the website, were also convicted on separatism charges and sentenced to between three and eight years in prison in December 2014.142

In August, Tibetan blogger Dawa Tsomo was detained “for violating China’s internet rules and regulations” after she had criticized the government’s mishandling of the welfare and living conditions of Tibetans still living in Kyegudo, the site of a devastating 2010 earthquake. Her whereabouts following the detention were unknown.143

Long-term detainees include 2010 Nobel Peace Prize winner Liu Xiaobo, who is serving an 11-year sentence on charges of “inciting subversion of state power” for publishing online articles, including the prodemocracy manifesto Charter 08.144 At least two Uyghur website managers, Memetjan Abdulala and Gulmire Imin, were jailed for life in the aftermath of ethnic violence in Tibet in 2008 and Xinjiang in 2009, when local courts—often after closed trials—imprisoned at least 17 individuals involved with websites that reported on Tibetan or Uyghur issues.145

Though the people imprisoned represent a tiny percentage of the overall user population, their harsh sentences have a chilling effect on the close-knit activist and blogging community and encourage self-censorship in the broader public. Trials and hearings lack due process, often amounting to little more than sentencing announcements, and detainees frequently report abuse in custody, including torture and lack of medical attention.146

Chinese authorities abolished the extrajudicial sentence known as reeducation through labor in 2013 after domestic calls for reform.147 However, individuals can be detained without trial under similarly

---

142 Celia Hatton, “China jails students of Uighur scholar Ilham Tohti,” BBC, December 9, 2014, http://bbc.in/1Lt7kQ.
poor conditions in drug rehabilitation and “legal education” centers. Internet users have also fallen victim to forced psychiatric detention. The whereabouts of at least one detainee, Li Qidong, who officials hospitalized in Liaoning in 2009 after he criticized the government in online articles, remain unknown.

State agents also abduct and hold individuals in secret locations without informing their families or legal counsel. In 2012, the National People’s Congress enacted an amendment of the Criminal Procedure Law that strengthened the legal basis for detaining suspects considered a threat to national security in undisclosed locations, among other changes. In response to public feedback, a clause was added requiring police to inform a suspect’s family of such a detention, though they need not disclose where and why the suspect is being held. Despite this improvement, the amendment maintained vague language that is open to abuse by police and security agents. In April 2014, the families of 17 Sina employees responsible for screening the company’s e-publication content were informed that the workers were abroad on business for a month, but a local news outlet reported in May that they had been detained. Dozens of human rights lawyers, including many representing clients in freedom of speech cases, disappeared or were held in undisclosed locations in 2015.

Surveillance, Privacy, and Anonymity

Users hoping to avoid repercussions for their online activity face a dwindling space for anonymous communication as real-name registration requirements expand online, among mobile phone retailers, and at public internet facilities. The authorities justify real-name registration as a means to prevent cybercrime, though experts counter that uploaded identity documents are vulnerable to theft or misuse, especially since some verification is done through a little-known, government-linked contractor.

In 2012, the National People’s Congress Standing Committee approved new rules to strengthen the legal basis for real-name registration by websites and service providers. The rules threatened violators with “confiscation of illegal gains, license revocations, and website closures,” largely echoing the informal arrangements already in place across the sector. Comment sections of major news

---

153 Danny O’Brien, “China’s name registration will only aid cybercriminals,” Committee to Protect Journalists blog, December 28, 2012, [https://cpj.org/x/5177](https://cpj.org/x/5177).
ports, bulletin boards, blog-hosting services, and email providers already enforced some registration. The MIIT also required website owners and internet content providers to submit photo identification when they apply for a license, whether the website is personal or corporate. Nevertheless, the 2012 rules extended regulation to the business sector who must gain users’ consent to collect their personal electronic data, and outline the “use, method, and scope” of its collection. The rules offer no protection against law enforcement requests for these records.

Microblog providers have struggled to enforce identity checks. Online reports of Sina Weibo users trading defunct identification numbers to facilitate fake registration indicated that the requirements were easy to circumvent. Sina’s 2014 report to the U.S. Securities and Exchange Commission noted the company’s exposure to potentially “severe punishment” by the Chinese government as a result of its noncompliance. Implementation of the real-name policy also makes it harder for the state’s hired commentators to operate undetected. One study reported officials encouraging commentators to use pseudonyms and fake documents to hide their affiliation with the propaganda department.

In summer 2014, the SIIO issued interim rules for anyone “employing instant messaging tools as public information services,” requiring service providers to verify user identities and register them with a government agency.

In January 2015, the SIIO announced that the government would truly begin enforcing real-name registration on all websites beginning on March 1. Alibaba Group Holding Ltd., Tencent Holdings Ltd., Baidu Inc., Sina Corp. affiliate Weibo Corp., and other companies were reported to have deleted more than 60,000 accounts on various platforms because they did not conform to the new, stricter regulations.

A draft antiterrorism law was made public for consultation in November 2014. Among the provisions is a requirement for technology firms to provide the government with surveillance “back doors” and supply law enforcement agencies with encryption keys and user data. All online service providers and telecommunication companies would be required to store user data within China’s borders. As of May 2015, the draft law was still under deliberation. In late 2015, outside the coverage period of this report, news reports said Chinese officials were seeking backdoor access to the data of Chinese users in direct requests to American technology companies.

162 Han, “Manufacturing Consent in Censored Cyberspace.”
164 Paul Carsten, “China censorship sweep deletes more than 60,000 Internet accounts,” ed. Robert Birsel, Reuters, February 27, 2015, http://reut.rs/1AR2qeU.
Commercial Encryption dating to 1999, and related rules from 2006, already require a government regulator to approve encryption products used by foreign and domestic companies.168

Internet commerce is undermining online anonymity. Many users voluntarily surrender personal details to enable financial transactions on social media sites. Mobile phone purchases have required identification since 2010, so providing a phone number is a common way of registering with other services.169 One analyst estimated that 50 percent of microblog users had exposed their identification numbers to providers by 2012, simply by accessing the platform from their mobile phone.170 Though not consistently enforced in the past, a crackdown on real-name registration for existing mobile subscriptions began in early 2015.171

China’s “second generation” national ID cards—which are administered by police—are required to be digitally embedded with fingerprints; the first generation of cards became defunct in 2013.172 The State Council aims to link credit, social security, and other personal information to these biometric databases. Writer Mo Zhixu laid out some possible implications, saying “ID numbers culled online will soon become useless for repeated use”; “relatives and friends will not … dare, to lend their ID numbers to anyone else”; and “personal credit information will necessarily include information about internet use.”173 In 2013, a Uyghur blogger reported that he was unable to join a Weixin page about sports using his national ID number, which identifies his birthplace as Xinjiang; he was only able to register with the number of a Han Chinese friend.174

Chinese providers are required to retain user information for 60 days, and submit it to the authorities upon request without judicial oversight or notification of the user.175 In 2010, the National People’s Congress amended the State Secrets Law,176 obliging telecommunications operators and ISPs to cooperate with authorities investigating leaked state secrets or risk losing their licenses.177 An amendment to the Criminal Procedure Law that took effect in 2013 introduced a review process for allowing police surveillance of suspects’ electronic communications, which the Ministry of Public Security permits in many types of criminal investigation, but the wording of the amendment was vague about the procedure for the review.178

Privacy protections under Chinese law are minimal. In the words of one expert, the law explicitly au-
China

thorizes government access to privately held data, and “systematic access” to “data held by anyone” is a realistic possibility once e-government strategies are fully implemented.179

Real-name registration is just one aspect of the pervasive surveillance of internet and mobile phone communications in China. The DPI technology used for censorship can monitor users, and personal text- and instant-message exchanges have been cited in court documents. One academic study reported that when users entered blacklisted search terms on Baidu, their IP addresses were automatically sent to a location in Shanghai affiliated with the Ministry of Public Security.180 Cybercafes check photo identification and record user activities, and in some regions, surveillance cameras in cybercafes have reportedly transmitted images to the local police station.181 Given the secrecy surrounding such capabilities, however, they are difficult to verify.

As with censorship, surveillance disproportionately targets individuals and groups perceived as anti-government. In January 2015, the Xinjiang government issued a new regulation requiring real-name registration for Uyghurs attempting to purchase mobile phones, computers, and other electronic devices with storage, communication, and broadcast features. Stores selling such equipment are required to install software that provides police with real-time electronic records on transactions.182

Intimidation and Violence

Allegations of torture and extralegal harassment are widespread among Chinese detainees, particularly political prisoners, a category that encompasses the majority of freedom of expression cases. In May 2015, Human Rights Watch reported “physical and psychological torture during police interrogations, including being hung by the wrists, being beaten with police batons or other objects, and prolonged sleep deprivation” in a review of hundreds of ordinary criminal cases. “Political prisoners ... have experienced much of what is described in this report and often worse,” the report said.183

Internet users also risk being held under house arrest. In such cases, including the extralegal house arrest of poet Liu Xia (wife of Liu Xiaobo) since 2010, internet and mobile phone connections are often severed to prevent the individual from contacting supporters and journalists.184 While there are several cases of long-term house arrest, the circumstances and degree of confinement can be adjusted arbitrarily over time. Some groups attempt to monitor the number of dissidents known to be held under house arrest, but there are no statistics showing how many were targeted specifically for online activity.185

Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically as being “invited to tea.”186 Activists have also been

instructed to travel during sensitive political events, effectively keeping them away from their normal online and offline activities.

In July 2015, at least 159 lawyers were interrogated, detained, or disappeared. One human rights lawyer, Wang Yu, reported on July 9 that her internet service and power had been cut off, and shortly thereafter, that people were trying to break into her home. She remained in incommunicado detention as of October.  

Technical Attacks

China is a global source of cyberattacks, accounting for 41 percent of the attack traffic observed worldwide by Akamai in 2014. The survey traced the attacks to computers in China using IP addresses, meaning the machines themselves may have been controlled from elsewhere.

Even attacks found to have originated in China can rarely be traced directly to the state, but the scale and targets of the illegal cyber activity have led many experts to conclude that Chinese military and intelligence agencies either sponsor or condone it. The geographically diverse array of political, economic, and military targets that suffer attacks reveal a pattern in which the hackers consistently align themselves with Chinese national goals. In 2015, China-based attacks targeted international companies including Google, Yahoo, Microsoft, and Apple.  

Hackers, known in Chinese as heike (dark guests), employ various methods to interrupt or intercept online content. Both domestic and overseas groups that report on China’s human rights abuses have suffered from distributed denial-of-service (DDoS) attacks, which temporarily disable websites by bombarding host servers with an unmanageable volume of traffic. From March 25 to March 31, 2015, the hosting service GitHub faced a DDoS attack that crippled its services. Sources indicate that the assault originated in China. The monitoring organization Citizen Lab analyzed the incident and found that “while the attack infrastructure is co-located with the Great Firewall, the attack was carried out by a separate offensive system, with different capabilities and design, that we term the ‘Great Cannon.’ The Great Cannon is not simply an extension of the Great Firewall, but a distinct attack tool that hijacks traffic to (or presumably from) individual IP addresses, and can arbitrarily replace unencrypted content as a man-in-the-middle.”

In March 2015, it was revealed that the CNNIC was issuing false digital security certificates for numerous domains, including several owned by Google. This security breach allows for man-in-the-middle (MITM) attacks, in which attackers can impersonate the site for which the certificate was intended, thus acquiring personal and private information. Yahoo faced a MITM attack during

---

China

the 2014 Hong Kong protests,\textsuperscript{193} and Microsoft Outlook faced one in January 2015.\textsuperscript{194} In April 2015, Google and Mozilla both announced that they would revoke authority of root certificates belonging to the CNNIC,\textsuperscript{195} meaning that sites with those certificates would not be recognized by the browsers, potentially interrupting users’ connections to a range of sites, including banks and e-commerce platforms.\textsuperscript{196}

Another well-documented tactic is spear-phishing, in which customized email messages are used to trick recipients into downloading malicious software by clicking on a link or a seemingly legitimate attachment.\textsuperscript{197} Tibetans, Uyghurs, and others subject to monitoring are frequently targeted with emailed programs that install spyware on the user’s device.\textsuperscript{198} Other cyberattacks affect the broader population.\textsuperscript{199}

\textsuperscript{195} Lucian Constantin, “Like Google, Mozilla set to punish Chinese agency for certificate debacle,” PC World, April 2, 2015, \url{http://bit.ly/1jxt7IX}.
\textsuperscript{196} Dan Goodin, “Google Chrome will banish Chinese certificate authority for breach of trust,” ArsTechnica, April 1, 2015, \url{http://bit.ly/1Hlskkg}.
\textsuperscript{198} Dylan Neild, Morgan Marquis-Boire, and Nart Villeneuve, “Permission to Spy: An Analysis of Android Malware Targeting Tibetans,” research brief, Citizen Lab, April 2013, \url{http://bit.ly/1OvBOAO}.
\textsuperscript{199} “Recent Data Breach Events in China,” Privacy and Information Security Law Blog, December 31, 2013, \url{http://bit.ly/1hDw3CI}.
Colombia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>Free</td>
<td>Partly Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>14</td>
<td>16</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>30</td>
<td>32</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

| Population:                           | 47.3 million |
| Internet Penetration 2014:            | 53 percent   |
| Social Media/ICT Apps Blocked:       | No           |
| Political/Social Content Blocked:    | No           |
| Bloggers/ICT Users Arrested:         | No           |
| Press Freedom 2015 Status:           | Partly Free  |

2014 2015

Population:

| Obstacles to Access (0-25)             | 8    | 8    |
| Limits on Content (0-35)               | 8    | 8    |
| Violations of User Rights (0-40)       | 14   | 16   |
| TOTAL* (0-100)                         | 30   | 32   |

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- Gonzalo López, who was convicted of libel in February 2014 and sentenced to 18 months in jail for a comment posted on a newspaper’s website, exhausted all possibilities of legal remedy in April 2015 after the Supreme Court rejected his appeal and the Constitutional Court did not select the case for review (see Prosecutions and Detentions for Online Activities).

- In April 2015, the Supreme Court convicted and sentenced two former public officials responsible for the illegal interception of the communications of high court judges, journalists and opposition leaders. Nevertheless, intelligence agencies continued to operate with little oversight during the coverage period, and civil society groups raised concerns about illegal and excessive surveillance (see Surveillance, Privacy, and Anonymity).

- In August 2014, the Prosecutor General’s office cited lack of transparency and oversight in ordering a halt to the development of the Single Platform for Monitoring and Analysis (PUMA), a centralized government surveillance platform slated for use by the national police (see Surveillance, Privacy, and Anonymity).

- In January 2015, Facebook and mobile carrier Tigo launched the commercial initiative Internet.org, which offers users free access for two months to some internet content and services. Although it promises to expand access to some online content, critics have raised concerns that it violates net neutrality (see Media, Diversity, and Content Manipulation).

1 Internet.org changed its name to Free Basics in September 2015
Introduction

Despite steady improvement over the last five years, significant challenges still hamper widespread internet access in Colombia. The main obstacles are poor infrastructure, lack of development, and high costs. When users manage to surmount access and affordability issues, however, they are able to view and disseminate content relatively freely on the internet. Although there are occasional cases of content removal, takedowns are isolated rather than systematic and stem mostly from muddy legislation rather than onerous governmental policies. In a concerning development, 2014 marked the first case in which an online user received a jail sentence under Colombia’s defamation laws, although he was ultimately avoid jail time based on provisions in Colombian law that take into account prior record and sentence.¹ While prosecutions for dissemination of content online are still rare, exceptionally harsh penalties for minor copyright violations and criminal penalties for defamation constitute serious violations of user rights.

Additional challenges to user rights come in the form of violence and impunity. For the past five decades, the Colombian government, various paramilitary groups, and the FARC (a guerrilla group with leftist origins), have been engaged in armed conflict. Despite ongoing peace talks between the government and the FARC since 2012, high levels of insecurity persist. In this context of violent crime, at least sixteen journalists have been murdered and many more have been threatened since 2005, with little response from the judiciary.² Self-censorship both online and offline has become a prophylactic measure against such threats, particularly in rural areas where violence and impunity are more pervasive than in cities.

In late 2014 and early 2015, convictions in trials resulting from surveillance scandals set an important precedent for punishing police, military, and government officials engaged in illegal surveillance. The Supreme Court found Bernardo Moreno, former secretary of the president’s office, and María del Pilar Hurtado, former director of the government’s now-defunct Administrative Security Department (DAS), guilty of illegal interception of communications against high court judges, journalists, and opposition leaders.³ In February 2015 the politically-connected hacker Andrés Sepúlveda pled guilty to similar charges in another surveillance scandal involving interception of the communications of representatives in the peace talks between the FARC and the government in Havana.⁴

Issues of internet access and net neutrality also came to the forefront of debate in Colombia, prompted by the expansion of zero rating programs. In January 2015, Facebook launched its Internet.org service, which provides free access to Facebook and some other applications for subscribers to Colombian mobile carrier Tigo.⁵ Although zero-rating programs have been permitted by Colombian law since 2011 and implemented by some carriers since that time, Internet.org is notable for its scope and for the significant media debate it triggered. Proponents argue that the increased access

---

³ “Condena de 14 años para Hurtado y 8 para Bernardo Moreno por chuzadas,” [Sentence of 14 years for Hurtado and 8 years for Bernardo Moreno for ‘Chuzadas’] El Tiempo, April 30, 2015, http://bit.ly/1biN0yV.
to limited services is better than no services at all, but some NGOs and technology experts have raised concerns about the potential of the program to increase the digital divide and undermine the net neutrality principle.

In recent years, Colombian NGOs—namely the Foundation for Freedom of the Press in Colombia (FLIP), Fundación Karisma, Dejustica, Colnodo, and, lately, the Colombian Jurists Commission (CCJ)—have begun calling for more information regarding the scope of government surveillance and threats to user privacy, issues that will likely gain greater traction in Colombia as internet use becomes more widespread. NGOs have also begun campaigning about internet-related issues unfolding in the public debate, such as online privacy, net neutrality, the quality of mobile internet, and online copyright enforcement.

Obstacles to Access

Although internet penetration has steadily increased, Colombia still faces obstacles to access primarily stemming from socioeconomic factors. The lack of basic utilities and affordable internet access constitutes an informal barrier to information and communications technologies (ICTs). The implementation of zero-rating programs such as Facebook’s Internet.org may increase access to a selection of online platforms, but critics worry that it may also aggravate Colombia’s digital divide and weaken the application of the net neutrality principle.

Availability and Ease of Access

Internet access has increased steadily in Colombia over the past decade. According to the most recent figures from the International Telecommunication Union (ITU), Colombia’s internet penetration rate reached 53 percent by the end of 2014, compared to 52 percent in 2013 and 30 percent in 2009. Nevertheless, with nearly half of the population still without internet, significant obstacles to access remain. Lack of infrastructure in rural areas, low levels of digital literacy, and high prices all stand in the way of widespread access.

Internet access is facilitated primarily by DSL and cable connections. Colombia’s average internet speed is 3.7 Mbps—a figure that places it between Brazil and Argentina in a regional comparison. Many Colombian internet users access the internet outside of their homes, and cybercafes and education centers play a key role in expanding access. Twenty percent of internet users accessed the internet through cybercafes and 26 percent through education centers, while free public access points served a negligible percentage of internet users.

Colombia’s mobile penetration rate reached 113 percent at the end of 2014, and mobile phones are increasingly used to access the internet. Mobile connections range from basic data plans to full ac-

---

8 For comparison, Brazil had an average internet speed of 3.0 and Argentina had an average speed of 4.5 at the end of 2014. The global average speed was 4.5. Akamai, State of the Internet Visualization, Fourth Quarter 2014, http://akamai.me/1VdTuF5
access,11 but it is not clear if official measures of mobile internet penetration count restricted plans (i.e. access only to social networks) as mobile internet connections. Mobile internet is divided between subscription plans and pay-as-you-go plans. Of the roughly 5.6 million users (approximately 12 percent of the population) who have subscription plans, almost 4.9 million (approximately 10 percent) have high-speed mobile broadband subscriptions, 3G and above. The majority of mobile internet users have pay-as-you-go plans, which claim 21.4 million users (approximately 44 percent of the population). Of these users, 17 million (approximately 36 percent) have service of 3G or above.12

There is significant geographical disparity in internet penetration rates in Colombia. While the capital, Bogotá, has a fixed-internet subscription rate of 19 percent, the southern rural departments of Amazonas, Vaupés, Vichada, Guainía, and Guaviare have a rate of less than 1 percent combined.13 Only 4 to 5 percent of Colombia’s population lives in this region; however, the land accounts for approximately 55 percent of the country’s geographical area.14 Although many indigenous languages are spoken here, there do not appear to be significant efforts to offer online content in these languages. Even the official websites of Amazonas, Vichada, and Guajira—each of which lays claim to a large indigenous population—are in Spanish only, with no option to display them in any of the indigenous languages present in those territories.15

High internet prices and low levels of digital literacy also present substantial obstacles to internet access in Colombia. A 2014 Digital Consumers Survey revealed that 44 percent of people without internet in their homes cite high prices as the reason why they do not acquire the service, while 28 percent state that they do not think internet connection is necessary.16 The ITU’s scale of fixed-broadband prices lists Colombia as the 79th most affordable country out of 165 countries, placing it around the global median, with an average price of US$19.80 per month.17 For comparison, Colombia’s minimum legal monthly wage was set as COP 644,350 (US$260) for 2015.18 According to the ICT ministry (MinTIC), only about eight percent of people in the country’s lowest socioeconomic strata, which encompasses almost half the population, have subscriptions to fixed internet connections.19

The Private Council for Competitiveness, a national think tank devoted to exploring market competition, recommended decreasing internet and mobile prices between 20 and 40 percent in the next four years and pointed out that the high prices of internet and mobile communications are still obstacles to greater internet penetration.20 Official programs such as Vive Digital, implemented in 2010 and Colombia Aprende, the Education Ministry’s platform for the promotion of literacy, implemented in 2004, have begun breaking down barriers to digital literacy. Vive Digital, administered by the ICT ministry, aims to expand infrastructure, services, internet applications, and the number of Co-

---

11 DANE, Basic Indicators in ICT in Colombia 2014.
14 Based on DANE population projection for 2012 and the geographic area of the departments.
Colombia

Colombian internet users. Colombia Aprende also aims to expand the use of digital applications and devices, training some 16,000 teachers of digital literacy across the nation.22

Restrictions on Connectivity

No legal provisions impose connectivity restrictions in Colombia. The government does not place limits on bandwidth, nor does it impose control over infrastructure, except in emergency situations when internet service providers (ISPs) are required to make their infrastructure available for official response.23 In keeping with this lack of restriction, the government does not have centralized telecommunications infrastructure, nor has it established blocking protocols for instant, person-to-person communication, or tools to filter or block social media applications or content.

Colombia only has one internet exchange point (IXP), called “NAP Colombia,” through which ISPs exchange traffic to improve efficiency and speed. Located in Bogotá, the IXP is managed by the Colombian Chamber for Informatics and Telecommunications.24 Eighteen mostly privately owned telecommunication enterprises have direct connection with the IXP.

ICT Market

Colombia is home to 56 ISPs, and while 88 percent of the market is concentrated in the hands of four companies, there are nonetheless multiple market options from which to choose.25 Market entry is straightforward, and it is possible for anyone to establish an ISP by following the general requirements of the ICT Law (No.1341), which establishes free competition and prioritizes efficient use of infrastructure and access to ICTs.26

Registration requirements are neither excessive nor onerous. Business owners must provide personal and tax identification as well as a description of services, but no fee is required. This information is published in an open registry, and the ICT ministry then has 10 days to verify the data, after which the business may begin operating. Based on the required criteria, registration can be denied when information is incomplete or false, or when an ISP does not have the proper commercial status to offer such services.27 Service providers are obligated to pay a contribution of 0.01 percent of their annual income to an ICT Ministry Fund (Fontic) devoted to the development of nationwide ICT projects.28 ISPs must also apply for licenses to utilize the radioelectric spectrum, although there have been no complaints of difficulties or bias with this process.

The mobile landscape is more concentrated than the ISP market. Although Colombia has at least six mobile providers, two of those companies (Claro and Movistar) control two-thirds of the mobile internet market. This situation mirrors the mobile phone sector—although there are five providers, 82
percent of the market is in the hands of the two aforementioned companies. In 2009, the government declared that Claro occupied a dominant position in the market, which under Colombian law means that the company is subject to *ex ante* (prior) regulation on issues such as pricing and service bundling. The structure of the company, however, remains unchanged. As with ISPs, mobile service providers must also contribute 0.01 percent of their annual income to Fontic.

The ICT ministry establishes public selection mechanisms for mobile service providers. A 2013 spectrum auction resulted in two new players entering the market. While this is a step in the right direction, diminished market concentration has not yet been seen. In March 2013, the ministry renewed the spectrum licenses of Claro and Movistar for a new ten-year term without major alterations, suggesting that little is likely to change in terms of market dominance in the next decade.

### Regulatory Bodies

Colombia’s ICT sector is subject to numerous regulatory bodies, all of which are part of the executive branch of government and have varying but limited degrees of independence from the government. The three main regulatory bodies are the ICT ministry, the Communication Regulation Commission (CRC), and the National Spectrum Agency (NSA). The Superintendency of Industry and Commerce also has some control duties as part of its consumer protection obligations.

The president appoints the ICT minister, who oversees the telecommunications sector through the ICT ministry. The ICT minister also chairs the CRC, which is responsible for ensuring efficient service and promoting competition in the telecommunications sector and is formed by the minister and three commissioners who are also appointed by the president. The ICT minister designates the head of the NSA, which is the agency in charge of planning, management and supervision of the use of the radioelectric spectrum. While some have suggested that such an executive-driven design prevents objective oversight of the sector, affording the president a great deal of influence in its operation, to date, there are no clear examples of executive bias in rulings.

A 2014 OECD report proposed two principal suggestions for improving autonomy of regulatory bodies. First, the report recommended that the CRC develop more independence from Colombia’s central government because, as stands now, its board cannot deliberate without the presence of the ICT minister, and the ministry of finance fixes the agency’s budget. Second, the ICT ministry should refrain from regulating the sector, and focus solely on promoting the development and use of ICTs.

Since 2010, a government-appointed concessionaire has been responsible for allocating the .co domain. For the domains org.co, edu.co, mil.co, and gov.co, applicants must comply with specific requirements; for edu.co, for example, the applicant must be an educational institution.

---

31 Ley 1341 [Law 1341] art. 11.
34 Cortés, “Mobile Internet in Colombia - Challenges and Opportunities for Civil Society: The 2013 Spectrum Auction.”
Colombia

Limits on Content

No content is systematically blocked under Colombian law besides child pornography, which is blocked under laws that critics say are vague and overly broad. In addition, reports indicate that websites with content related to the FARC, a guerrilla movement that has been in armed conflict with the Colombian state since 1964, have been taken down or blocked with no explanation several times over the past years. Similar to offline media, online media in Colombia is subject to some content manipulation based on advertising revenue from government and private sources; however, online media outlets are able to exercise more independence from advertisers and government advertising revenue than offline media. Recent court cases have upheld the principle that intermediaries should not be held liable for content posted by third parties.

Blocking and Filtering

Blocking or filtering of content—other than child pornography—is not common in Colombia. However, the country has suffered from a violent conflict between the government, the FARC guerrilla group, and other paramilitary and guerrilla groups for over 50 years, and there have been sporadic reports of censorship of content disseminated by the FARC in recent years. Colombia, the United States, and the European Union recognize FARC as a terrorist organization, although several neighboring South American countries, such as Brazil, Argentina, Ecuador, and Venezuela, have not adopted that designation.

Although there are no legal restrictions on publishing materials about the ongoing conflict, FARC’s presence online has been subject to different forms of restriction. In 2012, for example, with the initiation of peace talks between the FARC and the Colombian government, FARC launched a music video on their website announcing their intentions to participate in the Havana Peace Talks. The site was blocked shortly thereafter. Content on FARC’s online accounts often consists of political or organizational propaganda rather than active recruitment or direct incitement to violence. Media coverage about censorship of FARC websites is scarce and the government has not commented on shutdowns of FARC websites or social media pages; therefore, it is not clear whether shutdowns of FARC websites are caused by technical blockings, cyberattacks, or result from decisions made by the organization itself, which operates in secrecy. Despite these instances, censorship of FARC websites does not appear to be systematic, and some FARC members have functional social media accounts.

According to the ICT ministry, the only content that is subject to blocking measures is child pornography. Decree 1524 (2002) requires ISPs to undertake technical measures to prevent the online availability of child pornography. In response to an information request, the ICT ministry stated that the criteria used to determine which content should be blocked are set every two years by a commission that includes the Colombian Child Care Office (ICBF), the Ombudsman, the National Prosecutor, and UNICEF. The Cybernetic Police Center of the Office for Criminal Investigation and the National Police’s Directorate of Criminal Investigation and Intelligence (DIJIN) evaluate reported

---

40 Communication from ICT Ministry in response to Request of Information Nº 661596 on February 24, 2015.
content and, if the content qualifies to be blocked, send the URLs to the ICT ministry, which in turn notifies the ISPs who ultimately block access to the sites. Anyone who feels adversely affected by the blocking measure may submit a complaint before DIJIN, which studies the case and decides to maintain or remove the blocking.

Although it is an important protection mechanism, the legal basis of the blocking procedure is somewhat murky, since neither of the laws restricting child pornography (Law 679 and Decree 1524) specify the process outlined by the ICT ministry. The possibility for civil or judicial oversight is limited because information about the websites blocked is classified, possibly out of fear that individuals would use circumvention tools to access child pornography sites if a list were made public.42

Content Removal

The Colombian government does not regularly order the removal of content, although periodic court cases have resulted in judicial orders requiring the removal of specific information deemed to violate fundamental rights. Some unconfirmed reports suggest that content produced by the FARC guerrilla group has been subject to removal or restriction. Members of the FARC have reported closure of social media pages, including restrictions on their Facebook pages and blogs.43 Meanwhile, Anncol (“the New Colombia News Agency”), which some political figures have denounced as an organization that supports FARC, has changed its top-level domain (TLD) on several occasions, allegedly because of diplomatic pressure exerted by the Colombian government on administrators of those TLDs to deregister the domain name.44

During the coverage period, cases pertaining to content disputes have exempted search engines from liability for posting links to content in their search results.45 One important recent ruling concerned the January 2013 case of Guillermo Martinez v. Google and the daily newspaper El Tiempo. In 1997, El Tiempo reported that Mr. Martinez was part of a mafia group. In 2003, charges against Martinez were dropped, but eight years later, when Martinez searched for his name on Google, the original allegation still appeared. In response to Martinez’s suit, the Constitutional Court ruled that Google was not responsible for the content of the journalistic pieces that were linked to the plaintiff’s name because Google is not an editor or a publisher,46 which suggests that the ruling may serve as a precedent to limit the liability of other intermediaries.

In May 2015, the court issued a second ruling that strengthened the precedent that search engines should not be held liable for links in their search results. The case arose from a writ for protection of fundamental rights (acción de tutela), which a citizen submitted to the Constitutional Court in 2013, requesting that the court order an online newspaper and Google to “erase any negative informa-

Colombia

In 2000, the woman had been implicated in a human trafficking investigation in relation to her work in a travel agency patronized by a man accused of human trafficking. Although she was investigated, her case reached the statute of limitations and she was never convicted. The newspaper *El Tiempo* published a note about the original case, but it did not publish anything signaling that her case had been dismissed; hence, the note violated the rights of good name and honor, according to the complainant.

In its 2015 decision, the Constitutional Court held that the media has a duty to update information regarding criminal cases until the case comes to an end. The Court ruled that *El Tiempo* must update the original note about the case to reflect that the complainant was not convicted and must use "robots.txt" and "metatags" to make the information harder to find in an online search. Finally, the Court did not order Google to de-index the information from its search results, on the grounds that search engines should not be liable for the information they index. The court also argued that liability for Google would violate guiding principles of an open internet like non-discrimination of content and harm free expression. The reception to the ruling was mixed among free speech and digital rights advocates. Although many praised the fact that it exempted intermediaries from liability, some worried that the ruling might place an excessive burden on the media. NGOs in Colombia have scheduled a variety of discussions over the next year to further assess the impact from this ruling.

Media, Diversity, and Content Manipulation

Colombia has a vibrant media environment with a number of digital media outlets and online spaces for political debate. Nevertheless, self-censorship is a notable problem for journalists in the realm of traditional media—and likely spills over into online media as well. According to a national survey of journalists conducted in 2013 by Proyecto Antonio Nariño (PAN), an alliance of organizations focused on freedom of expression and access to information, 47 percent of respondents reported that they avoided publishing information due to fear of aggression; 35 percent feared losing their jobs or having their media outlets closed; 25 percent feared pressure from state actors; and 60 percent believed that media outlets in their region modify their editorial positions in order to gain political favor.

The survey also revealed that 57 percent of respondents believe that local government pressures the media with allocation of government advertising. Given that financing is often extremely difficult, government advertising can make a significant difference in an outlet’s long-term existence. Although there are fewer detailed studies regarding the online environment specifically, one study from Javeriana University in 2012 found that at least 14 out of 61 online media outlets ran government advertisements. Although funding from the government, partisan, or corporate interests may

---

50 Although there are studies concerning self-censorship among journalists, to date, there are none concerning self-censorship among general internet users.
53 Germán Rey and José Luis Novoa, Medios Digitales En Colombia 2012, [Digital Media in Colombia] Centro Ático, Facultad
Colombia

manipulate online reporting, online media appear to have more independence from these funding sources, whereas in the traditional setting, official advertisement and favorable government relations are often a necessary condition for the continued operations of many offline outlets, especially in rural Colombian provinces.54

Many professional media enterprises thrive in Colombia’s largest cities and, in general, the government does not interfere with operations. Authorities do not issue official guidelines or directives on coverage to online media outlets or blogs, nor does the government employ or encourage individuals to defend official actions in online forums. Free or low-cost blogging services are available and are very popular. Along with Google, Facebook, YouTube, Yahoo, and Twitter, the Alexa ranking features Blogspot and Wordpress among the top 20 websites in Colombia.55

Net neutrality resurfaced as a topic of national debate in early 2015 when, shortly after being reelected, President Juan Manuel Santos proposed a National Development Plan that would exclude the net neutrality provision (Article 56) in place in the previous government plan.56 Concerned that Colombia would lose its legal protections for net neutrality, several civil society groups protested, and the article was ultimately preserved.57 Nevertheless, Colombia’s net neutrality law contains explicit exceptions for zero-rating programs, like Facebook’s Internet.org, which have also generated substantive debate among Colombian digital rights activists over the past year.

In January 2015, Facebook launched Internet.org through a partnership with the mobile carrier Tigo,58 making Colombia the first country in South America to adopt the program.59 Internet.org in Colombia offers users access to 16 applications for free for two months and was welcomed by the government as a catalyst for expanding internet access in Colombia.60 Media coverage has been favorable, stating that even though the program only provides access to a limited number of applications and not the whole internet, the program is better than no access at all.61 However, critics have raised concerns about user privacy on the program, as well as the fact that it may endanger the net neutrality principle because it divides users into those who can access an “internet” of a few selected platforms and those who have full access to the internet.

Although Colombia has regulations that prohibit filtering, the wording is vague and could lead to arbitrary practices. Law 1450 (2010) and Resolution 3502 (2011) stipulate that ISPs can make segmentation plans “according to the needs of the segment or the user,” which in practice allows them to offer plans in which the data consumption on certain applications (such as WhatsApp or Facebook)
Colombia

does not affect the contracted data limit. Mobile service providers offer several kinds of data plans, many of them obscure in terms of the network management being applied, as well as which kind of content and applications users may be charged for or that may affect data consumption. Fixed internet service is subject to the same transparency and regulation issues.

Digital Activism

The internet increasingly plays a central role in social movements in Colombia. A study from the NGO Somos Defensores (“We Are Defenders”) indicates that during the first decade of the 21st century, Colombian social movements used the internet primarily to display official information, but within the last five years, as the popularity of the internet has grown, these movements have embraced the online environment to campaign and investigate issues of interest to their members.

The most important example of online mobilization in Colombia occurred in 2008, with a rally against the FARC guerrillas known as “One Million Voices Against FARC – I am Colombia.” Oscar Morales, then a civil engineer, created a Facebook group to invite people to join the movement. Traditional media and government agencies quickly picked up the cause, which gave the rally significant exposure. According to media estimates, 12 million people in 200 cities worldwide took to the streets to call for a peaceful end to the conflict. In 2010, a similar rally was organized online, although with less impact. More recent mobilizations, such as peasants’ protests in the countryside and demonstrations against education and health bills, have also been organized online.

Violations of User Rights

Although prosecutions for online expression are rare in Colombia, two high profile cases in 2014 and 2015 attracted national and international criticism. In one case, the courts confirmed the conviction of an internet user who posted a comment criticizing a public official anonymously on a newspaper’s website, in the first online criminal defamation case in Colombia. Another user faces up to eight years in prison under Colombia’s excessively harsh copyright laws after he posted an academic article on the website Scribd. Although the government has taken some positive steps to prosecute illegal surveillance in recent years, evidence suggests that surveillance and violations of privacy remain widespread.

Legal Environment

Article 20 of Colombia’s National Constitution guarantees freedom of information and expression and prohibits prior restraint. This article was developed by the Constitutional Court in accordance with the standards of the Inter-American Court of Human Rights. Article 73 further provides for the protection of “the liberty and professional independence” of “journalistic activity.” Although there are no specific provisions protecting freedom of expression online, a blogger has the same liberties and protections as a print or broadcast journalist. The Constitutional Court confirmed the application of

---

65 Several decisions of the Constitutional Court state that Freedom of Expression is a universal right. See for example,
such protections to the internet in a 2012 ruling. In its decision, the Court stressed the Joint Declaration on Freedom of Expression and the internet, which states that “freedom of expression applies to the internet, as it does to all means of communication,” and that “restrictions on freedom of expression on the internet are only acceptable if they comply with established international standards... are provided for by law, and... are necessary to protect an interest which is recognized under international law [the “three-part test”].”

Despite the protections for free expression established in Colombian law, Colombia still has criminal penalties for defamation, which have been applied to online speech. According to the Colombian penal code, individuals accused of insult can face between 1.3 and 6 years in jail and a fine of between US$3000 and US$345,000, and individuals accused of libel can face between 1.3 and 4.5 years in jail, with the same possible fines. Although there are no penalties in place for libel, defamation, irresponsible journalism, or rumormongering that are specific to online content, cases pertaining to online defamation have occasionally been brought before the court with varying outcomes.

The courts have not applied the penal code’s provisions on libel and slander to third party intermediaries; however, the penal code includes a concerning provision regarding online publication or reproduction of insults against others. According to Article 222 of the penal code, “whoever publishes, reproduces, or repeats insult or libel” may also be subject to punishment. This article raises concerns as it leaves open the possibility for charges of indirect insult and libel. The following article in the penal code establishes the use of “social mediums of communication or of other collective divulgence” as an aggravating circumstance that can increase the penalty for insult or libel. The use of internet was considered an aggravating circumstance in the case against Gonzalo Hernán López (See Prosecutions and Detentions for Online Activities).

In July 2015, after the end of the coverage period for this report, two bombings in the capital city of Bogotá injured ten people. In the wake of the attacks, the Prosecutor General declared that anyone who shares photos or videos of possible terrorist attacks in publications or on social networks instead of surrendering the material directly to the authorities is subject to prosecution. The statement received widespread criticism since such prosecutions would lack legal basis and would entail a serious violation of the right to expression and information; however, no one has yet been prosecuted under this edict.

Prosecutions and Detentions for Online Activities

Prosecution, imprisonment, or detention for ICT activities is quite rare in Colombia, and writers, com-

---

Colombia

mentators, or bloggers are not systematically subject to imprisonment or fines as a result of posting material on the internet. Nevertheless, in a ruling that clearly violated international norms for freedom of expression, which state that criminal penalties should not apply in defamation cases, Colombian courts confirmed the first sentence for online defamation in July 2014. By applying Colombia’s criminal defamation laws to online speech, this ruling sets a concerning precedent for violations of user rights.

In February 2014, private citizen Gonzalo López was convicted of libel for using an anonymous profile to insult Gloria Escalante, the manager of a public utility company, in the comments section of the online version of the newspaper El País in 2008. Judicial police identified López through his IP address and seized two computers from his office. López, who called Escalante a “rat” and a “thief” in his comments, was the first Colombian to be convicted of libel for content posted online. He was sentenced to 18 months and 20 days in prison and issued a fine of COP 9,500,000 (US$4,700), although he did not serve jail time based on provisions in Colombian law that allow certain defendants to avoid imprisonment depending on their sentence and prior record.

López appealed the sentence, but the Supreme Court of Justice confirmed the conviction in July 2014. In October 2014, using a writ of protection of fundamental rights (acción de tutela), López again challenged the sentence for violating his right to freedom of expression, but his appeal was denied in February 2015. Finally, the Constitutional Court did not select the case for revision, which exhausts his options to overturn the conviction.

The outcome of López’s case differed from a previous case where the court acquitted a journalist for insult despite the fact that the complainant was a well-known and powerful politician. In July 2013, the Supreme Court overturned the conviction of Luis Agustín González for insult or slander. He was initially convicted by a lower level court for publishing an editorial that referred to a local politician as, “arrogant, humiliating, despotic, capricious, extravagant, and defiant.” Following an appeal from the politician, the Constitutional Court reopened the case in March 2014, but the complainant lost the appeal.

Colombia has harsh penalties for copyright violations and currently lacks the flexible fair use standards employed in many countries. In July 2014, the Colombian student Diego Gómez was charged with violating copyright violations for uploading an academic thesis onto Scribd. The author com-

74 Colombian law does not prohibit anonymity, so the fact that the post was anonymous did not influence the charges against López.
plained and pushed for a criminal prosecution. As of May 2015, the case was still ongoing. If convict-
ed, Gómez may face up to eight years in prison on top of substantial fines.79

In July 2014, the Superior Tribunal of Bogotá overturned the conviction of Joaquín Pérez Becerra, director of Anncol (“the New Colombia News Agency”), a Swedish-based news site that criticizes the economic and political policies of the Colombian government from a far left perspective. After being arrested while traveling through Venezuela, Becerra was brought to Colombia and convicted and sentenced to eight years in prison in 2012 on the charge of criminal conspiracy as an ally of the FARC guerrilla group.80 According to the prosecutor’s office, his work in the news agency served FARC’s interests and connected them with funds from his connections in Europe. After spending three years in prison, the higher tribunal ordered his release, saying that they could not find adequate evidence to support his conviction.81

Surveillance, Privacy, and Anonymity

During the coverage period, the courts sought to reign in illegal and excessive surveillance, passing down sentences to former public officials involved in a 2009 wiretapping scandal; meanwhile, the Prosecutor General ordered a halt in the development of a centralized surveillance platform being developed by the national police based on concerns that the platform lacked sufficient oversight. Despite this progress, however, concerns about illegal surveillance by certain sectors of the government and military persist, with investigative journalists continuing to uncover grave privacy violations by the police and military in 2014 and 2015.

While intercepting personal communications in Colombia is authorized only for criminal investigation purposes and legally requires a judicial order,82 service providers are required to collaborate with intelligence agencies by providing access to the communications history or technical data of any specific user without a warrant.83 Retention and treatment of user data by authorities other than the intelligence agencies and departments related to criminal investigation has not yet been regulated in Colombia. Colombian law also allows intelligence agencies to monitor the electromagnetic spectrum without a judicial order.84 An additional threat to user privacy comes in the form of Article 2 of Decree 1704 (2012), which requires that ISPs have backdoor access for criminal investigation purposes—which can be used under the Prosecutor General’s authorization.85 A service provider that does not comply with these obligations will face fines and could lose its license to operate.86

Colombia has no general restrictions against anonymous communication, and there are no registration requirements for bloggers, cybercafe owners, or users. However, the police have access to a database that must be maintained by telecommunication service providers. This database contains

86 Decreto Numero 1704 [Decree 1704], art. 7.
user data, such as name, ID number, place and residence address, mobile phone number and service activation date. 87 Users must provide accurate information under penalty of perjury, which is punishable by a minimum of six years in prison.88

Since 1993 Colombian law has banned the use of “communication devices that use the electromagnetic spectrum” to send “encrypted messages or messages in unintelligible language.”89 In response to an information request, the ICT ministry explained that those provisions apply only “to the content of the communications, not the encryption of the medium.” Despite of the ambiguous wording of the law, the ICT ministry further claimed that these provisions only apply to radio-like devices and not to the internet.90 The Intelligence and Counterintelligence Act stipulates that voice encryption service may be implemented “exclusively” for the intelligence agencies and “high government” officials by telecommunications service providers.91 Thus, mobile voice encryption is restricted for any citizen who is not part of the “high government” or intelligence agencies.

Although investigative journalists have sought to uncover surveillance practices, the scope of government and military surveillance in Colombia is still unclear. Apart from the occasional public bidding or contract that sheds some light on the matter, gaining an accurate picture of Colombia’s surveillance activities is very difficult. The lack of clarity regarding surveillance is aggravated by the fact that information related to intelligence activities is classified under Law 1621 (2012). Further complicating the matter, there is no independent body to oversee surveillance activities or to hold those in charge accountable. Congress receives a yearly intelligence report, but as there is no independent oversight, partial or biased information can be submitted.92

In July 2015, a hacker leaked 400 GB of documents from the Italian information technology company Hacking Team, which is best known for providing spyware to governments.93 Among these documents were emails suggesting that the Colombian government had contracts with the company, evidence that supports research published by Citizen Lab at the University of Toronto in early 2014.94 Leaked emails reference the National Police Office’s purchase of Hacking Team’s Remote Control System (RCS) called “Galileo,” which is capable of accessing and taking control of (hijacking) the target devices’ keyboard register, microphone and camera.

Although National Police have denied any direct relation with Hacking Team and have only admitted to contractual ties with a Colombian company called Robotec, which distributes Hacking Team’s services,95 the leaked documents indicate that the National Police contacted Hacking Team directly to activate spyware.96 Another leaked email suggested that the U.S. Drug Enforcement Agency (DEA)

88 The penal code outlines penalties for perjury of bearing “false witness.” Penal Code, art. 442
90 Communication Nº 811811, ICT Ministry to Karisma Foundation, April 27 of 2015.
93 Although this event occurred after the end of the coverage period for this report, it reflects the environment of surveillance over the past year in Colombia.
95 “Policía indicó no tener vínculos comerciales con firma Hacking Team,” [Police declares that there are no commercial links with Hacking Team] El Tiempo, July 8, 2015, http://bit.ly/1WnPXRJ.
Colombia

may be engaged in surveillance practices in Colombia. Although it is still unclear if Hacking Team software is currently being used by the National Police or U.S. DEA, and, if so, how it is being used, several Colombian civil society organizations criticized the excessive and apparently uncontrolled use of intelligence tools in the country, which they argue has been facilitated by “weak legislation” on intelligence matters.

Episodes of illegal surveillance (known in Colombia as “Las Chuzadas”), carried out by intelligence agencies, the army or the police, have constituted an ongoing scandal in Colombia in recent years. In February 2014, the Colombian magazine Semana exposed an illegal wiretapping operation carried out by the army against government representatives taking part in peace talks with FARC leaders in Havana, Cuba. According to the media, the military set up a fake internet cafe under the code name Andrómeda, which it used to illegally target government and FARC representatives. In addition to conducting illegal surveillance, the army also recruited hackers to illegally access communications between representatives on both sides of the peace talks.

In May 2014, in the midst of presidential election campaigns, Semana revealed a video in which Andrés Fernando Sepúlveda, who worked for the presidential campaign of Oscar Iván Zuluaga—a frontrunner against President Juan Manuel Santos—was seen discussing confidential information about FARC members participating in the peace talks and strategies to use that information during the campaign. It is not clear if Sepúlveda intercepted communications or paid for information from people participating in Andrómeda, but he eventually signed a plea bargain and was sentenced to 10 years of prison for illegal interception of communications and use of malicious software, amongst other charges.

In October 2014, reporters revealed that military intelligence services maintained a list of professional and personal email addresses of national and international journalists who had covered the peace talks between the Colombian government and FARC representatives, as well as personal email addresses of NGO members and foreign embassies diplomats. The purpose of the list is unknown. In early 2015 the military confirmed that they were conducting investigations and that some officials involved in the scandal were relieved of their duties, and five were removed entirely from the service.

The government has taken some steps over the past year to punish perpetrators of illegal surveil-

---

Colombia

lance, although it seems unlikely that these efforts have changed the overall environment for surveillance in Colombia, as intelligence agencies continue to operate with minimal oversight. On April 29, 2015, the Supreme Court sentenced Maria del Pilar Hurtado, former director of the government Administrative Security Department (DAS), and Bernardo Moreno, former secretary of the president’s office, to 14 and 8 years in prison, respectively, on charges of illegal interception of communication. Hurtado and Moreno carried out a secret wiretapping operation, exposed in 2009 by investigative journalists at the magazine Semana, in which the now-defunct DAS intercepted the private communications of journalists, politicians, and NGOs. Although the government dissolved DAS in 2011 in the wake of the scandal, many of the public officials who staffed the project were transferred to the National Intelligence Agency (ANI), the new federal security agency that replaced DAS. The large transfer of personnel between the DAS and ANI has engendered concern over the scope of the new agency’s activities.

In August 2014, the Prosecutor General’s office ordered the national police to stop development of a centralized platform for monitoring and analysis, known as PUMA, because of the lack of transparency and guarantees to its lawful use. Details about PUMA initially surfaced in June 2013, when journalists reported that the government was investing upward of US$100 million in a monitoring platform, which was to become operational by the end of 2014 and would provide the government with the capacity to intercept communications in real-time, extending to social media, email, telephone networks, and internet data traffic. Official reports identified PUMA as a “fundamental tool for criminal investigation to ensure public safety” and assured that it would not be used as a general intelligence-gathering apparatus. Skeptical of this assurance, the Prosecutor General’s office asserted in their 2014 decision that the only way in which PUMA may be deployed is under control of the prosecutor’s office. Nevertheless, it is not clear if the national police still have the monitoring equipment or it has been handed to prosecutor’s office. Recent Hacking Team leaks raise further questions, as they seem to indicate that PUMA may be up and running under the National Police.

Intimidation and Violence

Corruption, longstanding armed conflict and associated surveillance, and the war against drugs have become the greatest threats facing freedom of expression in Colombia—regardless of whether that expression occurs in print or online. According to the NGO FLIP, at least sixteen journalists have been murdered and many more have been threatened since 2005. These statistics represent a continuation of violence in a country that has seen at least 142 murders of journalists in the past four decades. Of these, 67 cases have already reached their statute of limitations, meaning that the victims’ families will never see justice. Impunity—a pervasive problem in Colombia’s judicial system—is ranked by the nonprofit PAN’s Freedom of Expression and Access to Information Index as one of the
Colombia

greatest threats to overall expression. Colombia has the third highest impunity rate on the Global Impunity Index of the Center for Studies on Impunity and Justice Institute.

Due to the country’s high level of violence, it is difficult to isolate deaths that have resulted specifically from online activity. One recent murder, however, appears to have been connected to online activism. In September 2013, lawyer Edison Molina was murdered in Puerto Berrio, Antioquia. Although there have been no significant advances in the judicial investigation, FLIP has suggested that Molina’s online activity, in which he denounced acts of corruption in local government, may have led to his murder.

Daniel Mejía, activist and director of the magazine Senxura, received a threat against his life and the life of his family in October 2014, allegedly for his reporting on illegal brick factories in Sogamoso, which he published through traditional and online media. Mejía alleges that the threats came from paramilitary organizations with the participation of a member of the military forces.

Colombia’s Ombudsman Office reported that more than 93 journalists were threatened between January to August 2014, though most worked offline. There is no broad trend of retaliation specifically for online content in Colombia, and in general, online journalists have not faced the same level of danger as print journalists. A high level of intimidation towards media and human rights defenders in general, however, creates a climate of fear that also affects online journalists.

Technical Attacks

Various types of cybercrime, including hacking, illegal interception and use of data, and the distribution and use of malware are criminalized under Law 1273, which was passed in 2009. Penalties range from 36 to 48 months’ imprisonment, along with fines. While phishing—the stealing of sensitive personal data via malware disguised as legitimate email—appears to be a significant issue in Colombia, most evidence of hacking and other interception has involved interagency spying and intelligence work carried out primarily by the government, the army, and other official bodies (see Surveillance, Privacy, and Anonymity).

In early 2014, following the army’s Andrómeda hacking scandal, President Santos publicly stated that Colombia’s cyber defense sector was sorely lacking, and announced the creation of a commission focused on strengthening national cybersecurity. Colombia then partnered with the Organization of American States (OAS) to develop two bodies—the Colombian Cyber Emergency Response

119 Gagne, “Journalists Increasingly Under Fire in Colombia.”
Colombia

Group (coICERT) and the Cyber Police Center (CCP)—in order to ensure the country’s cybersecurity.\textsuperscript{123} Despite the president’s recent emphasis on Colombia’s vulnerability to cyberattacks, there are few known cases of technical violence perpetrated by private actors.\textsuperscript{124} One year after the government announced its cybersecurity strategy with OAS support, digital rights activists continue to push for greater participation in reforming cybersecurity and the inclusion of human rights protections in the development of the cyber security agenda.\textsuperscript{125}

\begin{thebibliography}{99}
\end{thebibliography}
Cuba

Key Developments: June 2014 – May 2015

• Over the past year, the Cuban government has opened over 100 new internet access points, permitted the first public Wi-Fi, and reduced prices and increased speeds for internet access at state-run cybercafes. Despite these notable advances, Cuba continues to have some of the most restrictive internet access in the world (see Availability and Ease of Access).

• On December 17, 2014, United States President Barack Obama ordered the restoration of full diplomatic relations with Cuba and the opening of an embassy in Havana for the first time in more than 50 years. The new policies, approved by the U.S. Treasury and Commerce departments, have opened the way for U.S. telecommunications and technology companies to start offering services to the island (see ICT Market).

• In December 2014, the performance artist Tania Bruguera used internet platforms to promote a performance in the Plaza of the Revolution in Havana. Bruguera and several prominent bloggers and activists who expressed support for her project online were arrested and detained before the performance could take place (see Prosecutions and Detentions for Online Activities).

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>28</td>
<td>27</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>33</td>
<td>32</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>84</td>
<td>81</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 11.2 million

Internet Penetration 2014: 5-30 percent

Social Media/ICT Apps Blocked: Yes

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2015 Status: Not Free
Introduction

Cuba has long ranked as one of the world’s most repressive environments for information and communication technologies (ICTs). High prices, exceptionally slow connectivity, and extensive government regulation have resulted in a pronounced lack of access to applications and services other than email. Most users can access only a government-controlled intranet rather than the global internet, with hourly connection costs amounting to 10 percent of the minimum monthly wage. Although mobile phone penetration is on the rise, and access to the high-speed internet provided by the new ALBA-1 fiber-optic cable was finally extended to citizens in late 2013 via the opening of new “cyber points” or “navigation halls,” ICT access remains limited.

A historic event took place on December 17, 2014, when President Obama ordered the restoration of full diplomatic relations with Cuba and the opening of an embassy in Havana for the first time in more than half a century. The surprise announcement came at the end of 18 months of secret talks that produced a negotiated prisoner swap, including the release of Alan Gross, an American government contractor arrested in 2009 and sentenced to 15 years in a Cuban prison for trying to deliver satellite telephone equipment capable of cloaking connections to the internet. On April 14, 2015, after meetings between U.S. officials and a delegation of Cuba’s Foreign Ministry and a high-level meeting between Obama and Raúl Castro in Panama City during the Summit of the Americas, the Obama administration announced that Cuba would be removed from the list of states that sponsor terrorism.

President Barack Obama also announced that the administration would work with Congress to ultimately lift the trade embargo and other sanctions. Even with the embargo still in place as of mid-2015, the new policies opened the way for U.S. telecommunications companies to start offering services to the island. The normalization of relations between the two countries and the opening of ICT trade has eliminated the Cuban government’s ability to blame low levels of internet access on the blockade and has inspired optimism in many observers, who see this radical change in relations as an opening for information technologies in Cuba.

Cuba has taken some tentative steps to reinforce this optimism by improving internet access on the island. Over the past year, the government opened a number of new internet access points, which boast somewhat faster speeds and lower prices. After an initial experiment with the first free public Wi-Fi zone, the government opened 35 paid public Wi-Fi hotspots in June and July 2015.1 For Cuba this progress in increasing access is historic, but it is still just a drop in the bucket when it comes to alleviating the most draconian restrictions on internet freedom in the hemisphere. Home internet connections are still forbidden, and even with reduced prices, public internet access points still cost US$2 per hour to use, which is equal to one-tenth of the average monthly wages. Even for those who might be able afford internet at new access points, the supply of internet access, mostly concentrated in the capital, is grossly out of proportion with the needs of a country of 11 million people.

Now the Cuban government faces increased pressure from its own citizens and the international community to expand access to an uncensored internet. However, the optimism derived from normalization of relations with the United States and the increasing number of internet cafes may be premature. Many worry that the official Cuban policy is inspired by the example of China and that new infrastructure will not mean an end to controlled and filtered access.

---

1 This event occurred outside the coverage period for this report.
Obstacles to Access

Access to the global internet in Cuba is extremely restricted, due to high prices and government regulation of access points. Many users are instead relegated to a tightly controlled government-filtered intranet and related email service. Nevertheless, over the past two years, important openings have taken place and more Cubans have gained access to the global internet or to other channels for sharing information with fellow citizens. Email access via mobile devices has been enabled and the first public Wi-Fi hotspots set up. Hundreds of new state-run access points, called “navigation halls,” have also been established, where internet speeds are relatively fast by Cuban standards, enabling multimedia engagement that was previously impossible. Penetration rates and internet speeds remain the lowest in the region and access is unaffordable for most Cubans, but a thawing in U.S.-Cuban relations has fueled optimism that ICT connectivity will further improve in the coming years.

Availability and Ease of Access

The latest data from the International Telecommunication Union (ITU) places Cuba’s internet penetration at 30 percent as of 2014, up from 28 percent in 2013 and only 14 percent in 2009. Meanwhile, the most recent data from the Cuban National Statistics Office reports a near tripling of registered .cu domain between 2012 and 2014. This increase may reflect the growing use of websites by companies after laws permitting private sector businesses were liberalized. These numbers, however, include users who can only access the government-controlled intranet.

Experts estimate that only a relatively small percentage of Cubans periodically have access to the unrestricted global internet via government institutions, foreign embassies, expensive connections in some hotels, and black market sales of minutes by those permitted to have online accounts. A small subsection of the general public can also access the global internet by going to the first free public Wi-Fi access point in the entire country, which was opened in January 2015 in the art studio of Cuba’s visual artist Alexis Leyva, better known as “Kcho.” Kcho received permission from the state-owned Telecommunications Company of Cuba S.A. (ETECSA) to provide free Wi-Fi access to his internet connection as part of a socio-cultural project offered by his studio. This initial experiment with public Wi-Fi was a harbinger for new developments: in June and July 2015, the government opened an additional 35 paid public Wi-Fi points in urban centers.

Select categories of users are authorized to access a broader, but still limited, portion of the global internet or other ICT tools. Cuban officials, doctors, or trusted journalists and intellectuals can legal-
Cuba

ly connect to an ISP in their offices, although their approved access—through the online network Infomed—is usually limited to email and sites related to their occupations. Resolution 92/2003 prohibits email and other ICT service providers from granting access to individuals who are not approved by the government, and requires that they enable only domestic chat services, not international ones. Entities that violate these regulations can be penalized with suspension or revocation of their authorization to provide access. Users may also face penalties if they violate the terms of authorization: In February 2015, the government canceled the Infomed national browsing and email service for some doctors and dentists because their emails had been used to publish classifieds on the popular website Revolico (a service similar to the U.S.-based Craigslist and one known for listing products on the black market).

For years, the rest of the Cuban population was relegated to no internet access at all or to a highly filtered government-controlled intranet, which consists of a national email system, a Cuban encyclopedia, a pool of educational materials and open-access journals, Cuban websites, and foreign websites that are supportive of the Cuban government. The intranet could be accessed through government-run internet access centers, the offices of Cuba’s only telecommunications provider, the Telecommunications Company of Cuba S.A. (ETECSA), or state-run cybercafes. Although most foreign websites are now available at these state-run access sites, the cost of accessing non-Cuban sites remains much higher.

Public access to the internet expanded somewhat after the connection and activation in 2013 of ALBA-1, a 1,600 km high-speed undersea cable stretching between Cuba and Venezuela, although not as impressively as many had hoped. Broadband service has become selectively available on the island at government offices and state-owned access points, but not for home connections. In June 2013, citizens began being able to access the internet through broadband connections to the new fiber-optic cable at 118 government-run “navigation halls.” In January 2015, officials announced plans to open 136 more internet access centers around the country by year’s end. As of mid-2015, there were 261 navigation halls (166 are ETECSA locales and 95 are in youth-centers, known as Joven Clubs).

The government has also cut prices for internet access points. In February 2015, ETECSA temporarily reduced the hourly charge for using the internet at state-run cybercafes and navigation halls from US$4.50 an hour to US$2.00 per hour, though this still amounted to roughly 10 percent of the average monthly salary. For a much lower fee of US$0.60 an hour, Cubans can access domestic websites. The price cut received little attention in the state media and news instead spread by word

---

8 According to the resolution, “Cuban websites that offer e-mail services cannot implement the creation of e-mail (Webmail) via an automatic process for natural persons or entities that are not duly authorized.” Legislación para el Sistema Nacional de Salud, Resolución Ministerial No 92/2003, July 18, 2003, http://bit.ly/1hi5xjD.
11 “Cuba First High-Speed Internet Connection Activated”; BBC, January 24, 2013, http://bbc.in/80qoQOM.
14 The price cut was initially set to last only until April 2015; however, sources in Cuba report that reduced prices have continued. Associated Press, “Cuba lowers prices to Internet access: now an hour costs 10% of monthly salary,” Fox News Latino, February 19, 2015, http://bit.ly/1G73BiB.
16 Jose Manuel, “Entrevista a viceministro del Ministerio de Comunicaciones (+Video),” delmonte1986 (blog), May 29, 2013,
Cuba

of mouth, but the impact on the number of users remains to be seen. ETECSA later announced that the lowered price would go into longer term effect beginning July 1, particularly at the 35 new Wi-Fi access points that were opened in parks and other public venues around the island in mid-2015.17

Users pay for government-run internet service directly at navigation halls or by purchasing a “Nauta” card (a pass that links to ETECSA’s interface of the same name that can only be used at specific locations), which allows them to access temporary accounts, valid for 30 calendar days as of the date of the first session. They are also able to open permanent accounts upon request, complete with username, password, and email address, if they can afford the cost of the service—and the high level of surveillance associated with such accounts. ETECSA monitors the accounts and retains the right to end a user’s access for a sweeping range of violations (see Surveillance, Privacy and Anonymity).

Users at the new navigation halls report being pleasantly surprised by the relatively high connection speed (for Cuba)—from 512kbps to 2 Mbps—enabling limited content streaming.18 Most Cubans continue to face extremely slow internet—and intranet—connections of up to 1 Mbps, making multimedia use nearly impossible.19 This is due to weak domestic infrastructure and the limited extension of access to the high-speed cable. According to one blogger’s account, users at navigation halls can access foreign news sites like the BBC, El País, and the Financial Times, as well as Miami-based El Nuevo Herald and Diario de las Américas if they can afford the higher fees for international websites.20 However, sites such as Radio/TV Martí, the U.S. government broadcaster that transmits to the island, remain blocked (see Limits on Content).

The Cuban government continues to control the legal and institutional structures that determine who has access to the internet and how much access will be permitted. Home connections are not yet allowed for the vast majority of Cubans, and the government regulates the sale and distribution of internet-related equipment. In early 2008, after a nearly decade-long ban, the government began allowing Cubans to buy personal computers, but prohibitively high costs place computers and internet access beyond the reach of most of the population.21 Out of a country of more than 11 million people, the number of computers was only a little over one million, and, of these, only about half had connectivity.22 After an April 2015 bilateral meeting, one U.S. official told journalists that the Cuban government had pledged to expand home connections to 50 percent of the population and mobile internet connections to 60 percent by 2020.23 However, such an increase would require a significant infrastructure upgrade, prompting speculation among knowledgeable observers as to whether it is realistic.

The government claims that all schools have computer labs, but in practice, internet access is usually prohibited for students or limited to very short periods of access, certain email accounts, or supervised activities on the national intranet. In May 2015, the Minister of Higher Education announced

http://bit.ly/1QypqYU
19 Jack Karsten and Darrel M. West, “Cuba slowly expands Internet access,” Tech Tank (blog), Brookings Institute, July 2, 2015, http://brook.gs/1KDxLF.
20 García, “Internet in Cuba: A Success in Spite of Everything.”

237 www.freedomhouse.org
upcoming internet access for teachers, researchers, and students at four universities on campuses and in residences. But few details, such as information regarding the speed of the connection, were provided and implementation remains to be seen.

Although Cuba still has the lowest mobile phone penetration rate in Latin America, the rate is rising due in part to changes in government-imposed restrictions on telecommunications. By the end of 2014, approximately 2.5 million Cubans owned mobile phones, or about 22 percent of the population. As the number of mobile phone users has grown, the state-owned ETECSA has begun implementing small changes beneficial to users. In 2012, ETECSA eliminated fees for receiving phone calls from within Cuba, cut the cost of sending a text message (from US$0.16 to $0.09), and reduced the daytime cellphone rates from US$0.60 to $0.35 per minute. In January 2014, ETECSA also announced it will allow balance transfers on cards between prepaid users. In July 2014, ETECSA announced the minimum mobile phone service fee—which had been US$5 per month—would be eliminated.

Despite these positive developments and occasional promotions, the cost of mobile service is still too high for the vast majority of Cubans. The government’s strategy seems to be predicated on convincing Cuban exiles to pay for these services for their relatives in Cuba—viewed by many as an attempt to attract new funds. Since January 2014, friends and relatives living abroad can use an online service to pay the phone bills of users living on the island. Through this system of refilling credit on cell phones from outside the country, the Cuban diaspora (including more than one million Cubans residing in the United States, and 100,000 in Spain) covers all or part of the cost of cell phone use for their families in Cuba. According to the Miami-based Havana Consulting Group, 54 percent of mobile payments to ETECSA come from the Cuban diaspora.

Due to the second generation cell phone infrastructure, most mobile phone users are unable to browse the web, but it is possible to send and receive international text messages and images with certain phones. Moreover, a growing number of Cubans have more advanced smartphones, often gifts from wealthier relatives living abroad. In March 2014, a new Nauta service was launched, which allows users to send and receive emails on their mobile phones but only with a .cu email account. The cost of the service (US$1 per 1Mb of data transfer) is taken from the mobile phone’s credit rather than from the balance of the users’ Nauta internet account. Despite the fact that users can only activate this service at four locales in Havana and that it is still very expensive, it is the cheapest option for email to date and has quickly proven popular, with over 200,000 people signing up within the first three months. The high demand reportedly took ETECSA by surprise, con-

Cuba

tributing to an overburdened network and disruptions for those making voice calls or sending text messages.33

Phones that utilize Global Positioning System (GPS) technology or satellite connections are explicitly prohibited by Cuban customs regulations.34 Additional restrictions are placed on modems, wireless faxes, and satellite dishes, which require special permits from the MIC in order to enter the country.35 Nevertheless, some Cuban citizens have established wired or Wi-Fi-based local area networks to exchange information, mostly entertainment content in the form of games, music, and photos. The Cuban authorities appear to largely turn a blind eye to such efforts, but beginning in May 2014, news emerged of selective dismantling of these networks in some Havana neighborhoods.36 Since much of the content shared on these networks appears to be apolitical—often at the request of administrators—some observers speculated that the motivation for the crackdown might be economic, as the networks’ existence cuts into ETECSA’s profits.37

Restrictions on Connectivity

The backbone structure of the internet in Cuba is entirely controlled by the government, and state authorities have the capability and the legal mandate to restrict connectivity at will. At times of heightened political sensitivity, the government has used its complete control of the cell phone network to selectively obstruct citizens’ communications. All calls and SMS from dissidents’ cell phones are monitored and service is sometimes cut for those working as freelance or citizen journalists voicing views the government does not condone.38

ICT Market

The Cuban ICT market is entirely government controlled with two state-owned ISPs, one of which also owns the only mobile phone carrier in the country. Weak infrastructure and restrictions on private enterprise constitute obstacles to internet access. The reestablishment of full diplomatic relations with the United States in December 2014, along with the reopening of the U.S. Embassy in Cuba and President Obama’s decision to lift Cuba’s designation as a state sponsor of terrorism, however, have strengthened the prospect of an end of the U.S. embargo on Cuba and have raised hopes that open trade between the two countries will lead to greater competition in the ICT market.

While recent years have seen an expansion in the number of internet and mobile phone users, the ICT sector remains dominated by government firms. There are only two ISPs in Cuba: The Center for Automatic Interchange of Information (CENIAI) and ETECSA (sometimes called ENET). Both are owned by the state.39 Cubacel, a subsidiary of ETECSA, is the only mobile phone carrier in Cuba.

---

35 Cuban Customs Website (Aduana General de la Republica de Cuba).
39 The private-firm Telecom Italia previously held shares of ETECSA until February 2011, when the state-owned company Rafin S.A., a financial firm known for its connections to the military, bought Telecom Italia’s 27 percent stake for US$706 million.
In July 2014, *L’Express* magazine revealed that French telecommunications company Orange Digital Horizons signed a confidential agreement with ETECSA to develop communications in Cuba. This contract stipulates that Orange will offer its services, products and prices (phones and equipment) to the only local operator and share expertise. Furthermore, Orange committed to creating an institute in Cuba, dedicated to training in technologies and services with a focus on the Latin American region. Further details of the agreement remain unclear.40

The reestablishment of relations between the U.S. and Cuba has also raised the prospects for expansions in the ICT market. In meetings with the Ministry of Foreign Trade and Investment and ETECSA, U.S. government officials highlighted increased communication and the opening of ICT services as a central goal in the United States’ new approach to Cuba.41 President Obama’s plan for Cuban relations includes facilitating the expansion of travel and remittances to Cuba, authorizing the sale of communications devices, and allowing telecommunications providers to establish infrastructure and services in Cuba.42 Already, the U.S. government has loosened some restrictions in ICT commerce, even while other trade remains limited pending U.S. congressional action to lift the embargo.

The new policies of President Barack Obama approved by the Treasury and Commerce departments opened the way for U.S. telecommunications companies to start offering services to the island. In March 2015, the U.S. carrier IDT Corp reached an accord with the state monopoly ETECSA to provide direct international long distance calls.43 Companies whose services are closely related to internet use, like Mastercard, Airbnb, or Netflix, also announced their entrance into the Cuban market.44 Yet other companies had already expressed interest in the Cuban market even before the official change in U.S. policy: in June 2014, a team of top Google executives visited the island to promote open internet access.45 Some months later, Google announced the release of Chrome, Google Play, and the free version of Google Analytics to be downloaded from Cuban IP addresses.46

These changes come after a period of significant domestic changes in Cuba, as the government has begun to implement some limited market reforms. Restrictions on private enterprise were eased under the 2012 update of Cuba’s economic model. Although proposed reforms did not initially extend to liberalization of the communications sector,47 in November 2013, ETECSA announced that it would allow private workers to market local and long-distance telephone services to the population as self-employed communications agents. The agents may also sell prepaid cards for fixed and mobile telephone services and internet access.48 The Cuban government also began to allow the limited cre-

---

45 David Adams, “Google executives visit Cuba for first time to promote open Internet,” *Reuters*, June 29, 2014, [http://reut.rs/1iAm41n](http://reut.rs/1iAm41n).
47 Nick Miroff, “Cuba is Reforming, but Wealth and Success are Still Frowned Upon,” *Business Insider*, September 4, 2012, [http://read.bi/1OX6fPk](http://read.bi/1OX6fPk).
ation of private cooperatives by computer science graduates in 2012, but tight internet restrictions, along with prohibitively high computer and software pricing, resulted in a nonexistent official market, although a black market for such commodities exists.49

Regulatory Bodies

No independent regulatory body for managing the ICT sector exists in Cuba. In 2000, the Ministry of Informatics and Communication (MIC) was created to serve as the regulatory authority for the internet. Within the MIC, the Cuban Supervision and Control Agency oversees the development of internet-related technologies.50

Limits on Content

Cuban law places strict limits on free speech and outlaws independent media. Although many foreign news websites are accessible from internet access points, websites focused on Cuban news and websites from Cuban dissidents or expats are often blocked. Various institutions, such as universities, further restrict content, frequently blocking social media sites. Despite these restrictions, Cuba does not have the same level of technically sophisticated blocking that characterizes other highly restrictive internet environments, such as China. Instead, Cuba relies primarily on severely limiting access to internet. Many Cubans are nevertheless able to access online content by creating improvisational underground networks, setting up illegal antennas, and passing around USBs with content downloaded from the internet.

Blocking and Filtering

Rather than relying on the technically sophisticated filtering and blocking used by other repressive regimes, the Cuban government limits users’ access to information primarily via lack of technology and prohibitive costs. Restrictions on email in the workplace, however, have been growing in recent years, and dissident websites and blogs continue to be subject to periodic disabling or blocking. The wording of certain government provisions regarding content regulation is vague and allows for a wide array of posts to be censored without judicial oversight. Resolution 56/1999 stipulates that all materials intended for publication or dissemination on the internet must first be approved by the National Registry of Serial Publications.51 Meanwhile, Resolution 179 (2008) authorizes ETECSA to “take the necessary steps to prevent access to sites whose contents are contrary to social interests, ethics and morals, as well as the use of applications that affect the integrity or security of the state.”52

The websites of foreign news outlets—including the British Broadcasting Corporation (BBC), El País, the Financial Times, and El Nuevo Herald (a Miami-based Spanish-language daily)—are readily available in Cuba.53 However, dissident or independent news sites, such as Cubanet, Diario de Cuba,

50 For the website of The Ministry of Informatics and Communications see: http://www.mincom.gob.cu/?q=node/353
53 García, “Internet in Cuba: A Success in Spite of Everything.”
Cuba

Cuboencontro, Hablemos Press, and 14ymedio are restricted. The sites of some Cuban activists and dissident organizations based on the island, such as the Patriotic Union of Cuba (UNPACU), the Christian Liberation Movement (MCL), and the civic project Estado de SATS, are also blocked at most access points. Revolico, a platform for posting classified advertisements for products circulating on the black market also continues to be blocked.

Social-networking platforms such as Facebook and Twitter are sometimes blocked at certain universities and government institutions, but may be accessed—with consistent monitoring but varying reliability—from some cybercafes and hotels. Voice over Internet Protocol (VoIP), on the other hand, is blocked throughout the country. In recent years, the government also increased its control over the use of email in official institutions, installing a platform that restricts spam and specifically prevents the transmission of “chain letters critical of the government.”

Beginning in 2007, the government systematically blocked core internet portal sites such as Yahoo, MSN, and Hotmail. As of 2015, these sites remain blocked in some government institutions, although they are largely accessible from hotels. Cuban authorities also restricted access to Cuban and foreign websites that contained independent reporting or views critical of the government. Among the continuously blocked sites are the Voces Cubanas platform, which hosts approximately 40 blogs, including Yoani Sánchez’s award winning Generación Y. While most of these sites and international portals were unblocked without explanation in February 2011, many were re-blocked in 2012 and 2013. In both cases, the associated bloggers were subject to intimidation, resulting in self-censorship.

Blocking occurs not only at the national level but also at the level of various intranet networks and at the point of access centers. In March 2015, the Nauta intranet banned Larry Press’ blog, The Internet in Cuba, one of the best sources about the Cuban ICT sector. In January 2015, University of Computer Sciences (UCI) banned Fernando Ravsberg’s blog Cartas desde Cuba, which had been hosted on the BBC Mundo platform from 2008 to 2013 until becoming independent.

Content Removal

While ETECSA does not proactively police networks and delete content, there have been reports of bloggers removing posts after being threatened by officials for publishing views criticizing government actions. In March 2015, Yoani Sánchez’s blog 14yMedio, was removed permanently from the


59 “If you are reading this, you are probably not in Cuba,” The Internet in Cuba (blog), March 30, 2015, http://bit.ly/1Wzrbyj.


61 For examples, see: “Malestar por Cambio de Edificio del Partido Comunista en Camagüey,” [Upset over Change to
new government-sponsored blog platform Reflejos. Although the government said that there were no prohibited topics on the platform, which was open to all Cuban users, they required bloggers to register with information cards and prohibited the publication of unlawful or counter-revolutionary content. During the short time in which it was active, Sanchez’s blog published a variety of content that ranged from cultural commentary to recipes to opinion columns.\textsuperscript{62}

**Media, Diversity, and Content Manipulation**

Cuba has one of the most restrictive media environments in the world. The constitution prohibits privately owned media, and restricts any speech that is deemed counter-revolutionary. The government closely monitors users who post or access information online and delivers harsh penalties to those it perceives as dissidents. Demand for access to internet among the Cuban population, however, has led to elaborate underground networks of internet access. To try to combat access to popular websites, the Cuban government has launched copycat versions of many websites as well as a blogging platform, but these platforms remain under tight surveillance and control. A network of progovernment bloggers and social media activists often harass individuals who are critical of the government.\textsuperscript{63}

Despite the severe censorship in official media, some journalists have started using the internet to disseminate content that the official press is reluctant to publish. In May 2014, Yoani Sánchez launched an independent online news site, 14ymedio. Although the site is blocked in Cuba, the editorial team is able to post content by emailing it to friends abroad. Users access content from the site through proxies and offline versions that are shared by USB flash drives.\textsuperscript{64}

The cost of access to technologies that facilitate information sharing continues to be high, and the Cuban government has pursued individuals who violated telecommunications access laws. Government technicians sporadically “sniff” neighborhoods with their handheld devices in search of ham radios, satellite dishes and illegal networks. For example, in December 2012 and May 2014, the government shut down large illegal Wi-Fi networks in Havana.\textsuperscript{65} Nonetheless, many Cubans find ways to access restricted content, and a vibrant community of bloggers in Cuba utilizes the medium to report on conditions within the country.

Cubans are often able to break through infrastructural blockages by building their own antennas, using illegal dial-up connections, or developing blogs on foreign platforms. The underground economy of internet access also includes account sharing, in which authorized users sell access to those without an official account for one or two convertible pesos (US$ 1-2) per hour. Some foreign embassies allow Cubans to use their facilities, but a number of people who have visited embassies for this purpose have reported police harassment. There is also a thriving improvisational system

\begin{flushleft}
\textsuperscript{63} “Operation Truth VideoTranscript Elicer Avila and Yoani Sanchez,” Translating Cuba (blog), \url{http://bit.ly/1Oywlc5}.
\textsuperscript{64} Tiffany Pham, “How She Did It: Yoani Sánchez Launches Cuban News Outlet 14ymedio,” Forbes, November 30, 2014, \url{http://onforb.es/1yz5eDp}.
\end{flushleft}
of “sneakernets,” in which USB flash drives and data discs are used to distribute materials (articles, prohibited photos, satirical cartoons, video clips) that have been downloaded from the internet or stolen from government offices. 66

Faced with popular demand for videos, games, and online social networking, the government has tried to intercept this demand and direct it to government-controlled platforms. Following in the footsteps of other repressive regimes contending with a highly literate and digitally interested populace, the government has launched its own copycat versions of popular websites, such as Wikipedia, Twitter, and Facebook. This allows the government to direct citizens to closely monitored, censored versions of these platforms. In 2010 the government launched Ecured, a copycat version of Wikipedia, 67 and in 2013 they launched the social networking site La Tendedera, which is accessible from youth centers. 68 Most recently, the Cuban government launched the blogging platform Reflejos. 69

Digital Activism

Social media is so restricted that Cubans have not been able to organize large-scale campaigns around political objectives. However, new initiatives to create platforms for free speech and information access—such as the creation of the first public Wi-Fi network in the studio of artist Kho, with government permission, and the launch of a (still illegal) independent online journalism outlet—tested the boundaries of the government’s restrictions on speech over the past year (see Obstacles to Access and Media, Diversity, and Content Manipulation). Other attempts to provide a platform for free speech and information, however, were prevented by authorities.

In December 2014, in the aftermath of pronouncements by Barack Obama and Raul Castro about a rapprochement between Cuba and the United States, the performance artist Tania Bruguera published a public letter to the two presidents and the Pope in which she proposed relocating her 2009 performance Tatlin’s Whisper #6 to the Plaza of the Revolution, thereby offering an open mic to the Cuban citizenry to express their views about their country’s future. 70 Calling her project #YoTambienExijo (I Also Demand), she used social media platforms to promote her performance from outside the island and was supported by a number of dissident groups and opposition blogs. Upon traveling to Havana on December 26, however, she was summoned to a meeting with government officials and told that she did not have authorization for the performance. When she publicly stated that she intended to go ahead with the performance, she was detained by authorities, along with a number of other online and offline activists who expressed support for her project (see Prosecutions and Detentions).

Violations of User Rights

Cuba outlaws a wide range of speech deemed to be counter-revolutionary or a threat to the public

order. In recent years, the Cuban government has moved from issuing long, multiyear sentences to using short-term detentions as a means of harassing independent journalists and bloggers. During the coverage period, several prominent online journalists and activists were detained after expressing their support for an unauthorized performance art piece that was slated to be performed in Havana. As part of thawing relations with the United States, the Cuban government released Alan Gross, a former U.S. contractor who had spent over five years in prison for distributing outlawed communication technologies on the island. Gross reported suffering severe mistreatment and abuse in Cuban prison, a charge that has been echoed by other individuals who have been imprisoned for their online activity.

Legal Environment

The Cuban legal structure is not favorable to internet freedom. The constitution explicitly subordinates freedom of speech to the objectives of a socialist society, and freedom of cultural expression is guaranteed only if such expression is not contrary to the Revolution. The penal code sets penalties ranging from a few months to 20 years in prison for any activity considered to be a threat to the Cuban state or public order, including a provision that authorizes the state to detain, reeducate, or monitor anyone who shows a “proclivity to commit crimes” by violating the norms of the socialist society. Meanwhile, the Law to Protect Cuba’s National Independence and Economy (Law 88), passed in 1999, punishes any activity that threatens Cuban sovereignty or facilitates the U.S. embargo. Although the U.S. executive has stated a desire to lift the embargo, as of May 2015, it was still in place. Anyone who passes information to the U.S. government that could bolster the embargo can face up to 15 years in prison, while spreading subversive materials can incur a penalty of three to eight years in prison and collaborating with foreign media outlets is punishable by up to five years in prison.

In 1996, the government passed Decree-Law 209, which states that the internet cannot be used “in violation of Cuban society’s moral principles or the country’s laws,” and that email messages must not “jeopardize national security.” In 2007, a network security measure, Resolution 127, banned the use of public data-transmission networks for the spreading of information that is against the social interest, norms of good behavior, the integrity of people, or national security. The decree requires access providers to install controls that enable them to detect and prevent the proscribed activities, and to report them to the relevant authorities. Furthermore, access to the internet in Cuba generally requires identification, rendering anonymity nearly impossible.

Prosecutions and Detentions for Online Activities

Under Raúl Castro, the Cuban government appears to have shifted its repressive tactics from long-term imprisonment of bloggers to short-term extralegal detentions, intimidation, and harassment.
Bloggers are still routinely summoned for questioning, reprimanded, and detained. Reporters associated with independent online newspapers, including the outlet Hablemos Press, face significant harassment. The dissident group Cuban Commission for Human Rights and National Reconciliation reported more than five instances of independent online journalists and bloggers being detained or brought in for questioning between June 2014 and May 2015.

The most shocking case of mass arrests occurred in December 2014 and early January 2015 when the artist Tania Bruguera used the hashtag #YoTambienExijo to announce her plans to stage a critical performance artwork in the Plaza of the Revolution in Havana. After trying and failing to receive official approval for the performance, she publically stated her intent to continue with the performance anyway and was arrested on the morning of December 30, 2014. Several prominent reporters and activists, including the blogger Yoani Sánchez, the director of the civic project and website Estado de SATS Antonio Rodiles, and the photographer Claudio Fuentes, who expressed solidarity with Bruguera’s project, were also detained. Although Bruguera was released on December 31, 2014, her passport was confiscated and she was ordered to stay on the island pending indictment.

These detentions follow a trend in Cuba, which has seen an increase in the number of arrests and detentions of activists over the past two years. These arrests tend to increase surrounding key political and social events. For example, in January 2014, threats toward and arrests of dissidents and activists spiked significantly surrounding the Community of Latin American and Caribbean States (CELAC) summit. Although most individuals were released within hours, more than 3,000 arbitrary politically motivated detentions were reported in the three months surrounding the summit. The blocking of hundreds of cell phones owned by activists was also reported in the days leading up to the summit. Bloggers and online activists are often caught up in such crackdowns. Because it is difficult to distinguish between independent blogging and political activism in Cuba, however, it is often impossible to accurately pinpoint whether detentions were in retaliation for online speech specifically.

The government has also prosecuted individuals associated with underground cyber-networks. In 2012, the government opened a criminal investigation of two highly profitable cyber-networks illegally using ETECSA’s fixed and mobile networks. The defendants, who are being prosecuted for illegal economic activity and fraud, face fines coupled with sentences of three to ten years in prison. In May 2014, Cuban authorities raided and seized equipment from another underground Wi-Fi network with 120 members.

Committee to Protect Journalists (CPJ), After the Black Spring, Cuba’s New Repression, July 6, 2011, https://cpj.org/x/4472.
78 Daniel Trotta, “Cuban Dissidents say political arrests top 1,000 in February,” Reuters, March 3, 2014, http://reut.rs/1G7njuF.
83 Trotta, “Cuban Dissidents Say Political Arrests Top 1,000 in February.”
Cuba

Despite the continued policy of harassment and detentions of bloggers, online activists have seen a loosening of travel restrictions over the past two years,\(^\text{87}\) and the government recently released two prominent political prisoners. In December 2014, as part of negotiations with the United States, the Cuban government released the American USAID contractor Alan Gross, who had been held for over five years, on charges that he distributed illegal communications technology to Cubans.\(^\text{88}\) In July 2015, the government released the well-known blogger and writer Ángel Santiesteban Prats, who had been jailed on trumped-up charges since early 2013.\(^\text{89}\) Santiesteban was arrested in connection with his political views several times prior to his December 2012 trial. Such harassment increased after his creation of the blog *The Children No One Wanted*, in which he criticized the government. Santiesteban reported mistreatment and torture during his imprisonment.\(^\text{90}\)

**Surveillance, Privacy, and Anonymity**

Surveillance of ICTs in Cuba is widespread, and dissident bloggers are subject to punishments ranging from fines and searches to confiscation of equipment and detentions. Anonymity and encryption technologies are strictly prohibited in Cuba,\(^\text{91}\) and web access points, such as those found in cybercafes and access centers, are closely monitored and users are required to register with their identification information.\(^\text{92}\)

Despite constitutional provisions that protect various forms of communication and portions of the penal code that establish penalties for the violation of the secrecy of communications, users’ privacy is frequently violated. Tools for content surveillance are likewise pervasive. Under Resolution 179/2008, ISPs are required to register and retain the addresses of all traffic for at least one year.\(^\text{93}\) The government routes most connections through proxy servers and is able to obtain all user names and passwords through special monitoring software called Avila Link, which is installed at most ETECSA and public access points.\(^\text{94}\) In addition, delivery of email messages is consistently delayed, and it is not unusual for a message to arrive without its attachments.

---


Web use at “cyber points” and “navigation halls” remains tightly controlled. A recent decree from the Ministry of Communications reaffirmed the government’s continued monitoring of internet traffic, stating that ETECSA will immediately end a user’s access if he or she commits “any violation of the norms of ethical behavior promoted by the Cuban state.”

Users must show their national ID cards and sign an agreement stating that they will not use the service for anything “that could be considered ... damaging or harmful to public security”—a vague term that could presumably extend to political dissent.

If users attempt to send email with attachments, ETECSA’s own NAUTA interface system greets them with a pop-up window reminding them that “other people may see what you are sending” and asking if they wish to continue. Although the pop-up window is marked “Internet Explorer” and appears to be a real message generated by the search engine, several Cuban online users have said that they had never seen such a message when using internet cafes in Havana’s tourist hotels. Such claims suggest that ETECSA may have programmed computers at its new access points to prompt users as a reminder that the government is monitoring their online activities.

**Intimidation and Violence**

Although the majority of cases of physical violence against activists in Cuba appear to be in retaliation for public protests rather than online activity, prominent online users have faced violence from police forces, and users who have been jailed for extended periods of time report being mistreated and tortured. For example, in June 2014, a member of the state security reportedly attacked Roberto de Jesus Guerra, the founder of Hablemos Press, as he walked to an embassy office to file a story online. Guerra and his wife have also begun receiving anonymous death threats. Two individuals recently released from prison after being arrested for ICT-related activities—the prominent blogger Ángel Santiesteban Prats, who was jailed on trumped up charges, and the U.S. contractor Alan Gross, who was charged with distributing illegal communication technologies—reported that they had experienced severe mistreatment and abuse during their detention.

**Technical Attacks**

Technical attacks do not appear to be a primary method of censorship in the country; however, one prominent cyberattack gained significant international media attention over the past year. In May 2014, the online newspaper 14ymedio was hacked one day after it was launched. Users who tried to access the site were redirected to a site called Yoani$landia, which insulted the director of the outlet, Yoani Sánchez. The site was restored shortly after the hack.
Ecuador

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>Partly Free</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>37</td>
<td>37</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 16 million
Internet Penetration 2014: 43 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2015 Status: Not Free

Key Developments: June 2014 – May 2015

- In January 2015, President Correa launched a Twitter campaign against his online critics, encouraging his supporters to find and release personal information about anonymous users who criticized the government online. This led to an online confrontation that escalated to include hacking, trolling, and threats (see **Intimidation and Violence**).

- In February 2015, Congress passed and the president signed the Organic Law on Telecommunications. Among other provisions, this law establishes some net neutrality protections; however, some critics worry that the newly created telecommunications regulatory body may lack independence from the executive (see **Regulatory Bodies and Media, Diversity, and Online Content**).

- Introduction of 4G telecommunication services has increased access and lowered the price of internet services (see **Availability and Ease of Access**).
Ecuador

Introduction

Ecuador stakes out a contradictory position on internet freedom—on the one hand, the government has engaged in widespread campaigns to improve internet access and digital literacy, and has vocally supported foreign whistleblowers like Julian Assange and Edward Snowden.1 On the other hand, evidence mounted during the coverage period that Ecuador’s government engages in widespread surveillance of its citizens and uses restrictive laws regulating media to curtail investigative reporting and the independent press. Most notably, in 2015, Ecuador’s president Rafael Correa waged a highly public social media war against his critics.

Ecuador gained notoriety in international media in 2015 after the president called out three Twitter users and the Facebook page Crudo Ecuador (“Raw Ecuador”) for criticizing him.2 In his weekly television address, President Correa encouraged his followers to respond to these critics and to reveal anonymous users’ personal information. In the wake of this address, the users he targeted faced significant harassment, and several closed their social media accounts.3

Leaks over the past few years have hinted that Ecuador has invested heavily in technology to conduct surveillance on its citizens. In July 2015, many of these suspicions were bolstered when the Italian technology company Hacking Team suffered a cyberattack, which resulted in the leak of 400 GB of internal information and private emails. These emails showed contracts between Hacking Team and the Ecuadorian government, and provided evidence that the government may have targeted opposition figures for surveillance.4

During the coverage period, politically motivated content removal via the abuse of copyright take-down requests, progovernment troll centers, and heavy sanctions for private media under the 2013 Communications Law all continued to present obstacles to free expression. The digital sphere, however, remains vibrant. Social media use is common and new digital ventures were launched over the past year.

In 2015 the government passed the Organic Law on Telecommunications, which put in place a variety of positive measures, including provisions to expand access, systematize regulation, and protect net neutrality. Nevertheless, some critics have raised concerns that the new regulator established under the law will lack independence from the government, since it will fall under the authority of the executive branch.5

Ecuador continued to expand access to mobile internet and broadband over the past year. New initiatives to produce smartphones in the country, as well as expanded 4G access, hold promise for faster, more accessible service. Prices for 3G and 4G have also decreased and use of these services is expected to grow, especially in urban areas.

---

3 Gabriella Torres, “Ecuador President Rafael Correa’s Troll Warfare,” BBC Trending (blog), BBC, January 30, 2015, http://bbc.in/1Kk8HGU.
5 “Entrevista a Alredo Velazco sobre la Nueva Ley de Telecomunicaciones en Ecuador,” [Interview with Alredo Velazco about the new Telecommunications Law in Ecuador], Quinotpoder, February 13, 2015, http://bit.ly/1MKeQ1F.
Obstacles to Access

Internet access continues to increase in Ecuador, spurred in part by government projects to expand access and increase digital literacy. The expansion of 4G technology is expected to further increase access, as more Ecuadorians turn to mobile internet. Nevertheless, a marked digital gap remains. Many people in rural areas access a slower internet, or do not have internet access at all.

Availability and Ease of Access

Ecuador’s information and communications technology (ICT) sector has experienced notable growth in recent years due in large part to government efforts to expand access, such as Ecuador’s “Digital Strategy 2.0” plan, which sought to expand broadband access, improve infrastructure, and train citizens in digital technology.6 The introduction of 4G telecommunications services and lower prices for mobile internet also contributed to improved and expanded access. In May 2015, the Spanish telecommunications provider Telefónica announced completion of the longest underwater fiber-optic cable in the Caribbean. This cable will connect the United States and Ecuador, significantly increasing the capacity and speed of the internet in the latter. The fiber-optic cable represents part of a larger advance in infrastructure improvements in Ecuador: the country has expanded from 3,500 km of fiber-optic cable in 2006 to 45,000 km in March 2015.7

According to an Akamai report from the first quarter of 2015, Ecuador’s average internet speed is 4.1 Mbps.8 As of 2014, the International Telecommunications Union (ITU) measured internet penetration in Ecuador at 43 percent, a notable increase given that penetration was just below 25 percent in 2009.9 The Ecuadorian government provided alternate statistics for internet penetration in March 2015, claiming that 41 percent of the population has internet subscriptions but that over 87 percent are internet users.10 It is not clear what differences in methodology account for the discrepancy between the government’s figures and those of the ITU, although, the latter seems to be more in line with overall trends and averages for the region.

Broadband (commonly used in urban zones) and satellite connections (often used in rural areas) have become increasingly popular in recent years. According to statistics from the ITU, Ecuador’s broadband penetration reached 7.8 percent in 2014, up from 6.7 percent in 2013.11 The Inter-American Development Bank rates Ecuador 9th out of 26 countries in Latin America and the Caribbean in terms of broadband penetration, although it falls behind many of its neighbors in South America.12 Multiple internet subscription options, ranging from dial-up pay-per-minute plans to cable and satellite connections, are available.

---

11 International Telecommunication Union, “Individuals Using the Internet.”
Ecuador

The Ecuadorian government classifies mobile phones as luxury items and imposes quotas on their importation.\textsuperscript{13} Despite this, the country is home to an active contingent of mobile phone users, with over 16.5 million mobile subscriptions in 2014 and a penetration rate of 103.9 percent.\textsuperscript{14} According to the most recent national study, regional variations still persist, with the lowest number of subscribers found in the Andean highlands of Bolivar, and the greatest number in Pichincha, which counts Ecuador’s capital, Quito, among its cities. Mobile phone penetration also varies among income and education levels.\textsuperscript{15}

In February 2015, Claro, owned by América Móvil, and Movistar, owned by Telefónica, reached an agreement with the government that would allow them to use radio-electric spectrum to expand 4G services in exchange for paying the Ecuadorian government over US$300 million and improving 3G coverage.\textsuperscript{16} These services are expected to reach more individuals than previous, fairly limited, attempts to introduce 4G technology because mobile penetration rates are above 100 percent in Ecuador and both companies are leading mobile providers, with a combined market share of over 70 percent. Ecuador also began producing high-end mobile phones with 4G capacity in 2014 after the government eased restrictions on importing certain phone parts. These phones, which are expected to have maximum download speeds of 100 Mbps, have the potential to provide consumers with faster access and greater downloading and file-sharing capabilities.\textsuperscript{17}

Coupled with the expansion of 3G and 4G technology was a decrease in prices for mobile internet access, although prices still constitute an obstacle to access for many people. Fixed-line internet services at speeds of 3 Mbps cost an average of US$20 per month, whereas 10 Mbps subscriptions are available at a rate of approximately US$35-40 per month.\textsuperscript{18} Mobile internet subscriptions vary from US$15 for 250 MB of data to US$80 for 6 GB.\textsuperscript{19}

Although a digital divide exists between rural and urban areas, Ecuador has shown improvement in extending internet access to rural areas over the past two years through programs facilitated by the Ministry of Telecommunications (MINTEL). Ecuador’s state-run Infocentros—community centers with network access that began to be installed in June 2012—have trained more than 185,000 people in the use of digital technology, according to the Ministry of Telecommunications.\textsuperscript{20} They offer internet access in 491 parish communities, and also provide equipment to 7,541 students throughout the country. As of July 2014, the number of people using Infocentros was almost 3 million nationwide.\textsuperscript{21}

\textsuperscript{13} A June 2012 ruling (No. 67) issued by the Committee on Foreign Trade (COMEX) also imposes quotas on the importation of mobile phones. According to the edict, the limitation is predicated on preventing further environmental degradation resulting from residual mobile phone waste. See La HoraNacional, “Restricciones de Comercio Limitarán Acceso a Internet” [Trade Restrictions will Limit Access to the Internet], June 26, 2012, http://bit.ly/1NGYZ9e.


\textsuperscript{20} Ministry of Telecommunications, “Infocentros Comunitarios,” [Infocenter Communities],http://bit.ly/1iPMYxq.

\textsuperscript{21} Ministry of Telecommunications, “Infocentros Comunitarios,” [Infocenter Communities].
Ecuador

Mobile classrooms—which are intended to offer access to those without Infocentros nearby—have also proven successful, reaching 2,816 parishes and municipalities since the project’s June 2012 inception. In 2013, MINTEL received an award from the ITU in recognition of the success of its Mobile Classrooms Project. In March 2015, the Ministry of Education began to construct an additional 500 mobile classrooms that will service 1,300 students in the public school system.22

In addition to the mobile classrooms and Infocentros, cybercafes provide internet access to Ecuadorians at a rate of US$1 per hour. The amount of cybercafes has doubled since 2009, from 1,355 to 2,574 in May 2015, according to statistics from the government’s Agency of Regulation and Control of Telecommunications (Arcotel).23

**Restrictions on Connectivity**

Ecuador’s backbone is not highly centralized. The government does not place limits on bandwidth, nor does it impose control over infrastructure, although a new provision in the 2015 Organic Law of Telecommunications grants the government the power to takeover telecommunications services in times of national emergency.24 Some civil society groups have raised concerns about the scope of this provision.25

In June 2015, protesters against the government in Quito and Guayaquil encountered service problems. Explanations for these problems range from network saturation to the possible presence of cell phone jammers.26 Some Twitter users posted photos of what appeared to be cell phone jammers and cameras placed around the park near the protests,27 although these reports have not been confirmed. Opposition party leaders present at protests encouraged users to circumvent problems through the use of apps such as FireChat, which uses wireless mesh networks to send messages without an internet or cellular connection. Ecuador’s telecommunications regulator Arcotel did not provide any reports or issue press releases in response to the claims that the networks were disrupted during protests.28

**ICT Market**

Ecuador has approximately 22 internet service providers (ISPs). State-owned CNT dominates the fixed-line market, with over 57 percent of subscriptions. Grupo Tija (Suratel) and Claro (Ecuadortelecom) control the next biggest shares of fixed line access, with 12 percent and 9 percent respectively.29

---

24 According to article 8 of the law, “in case of aggression, armed international or internal conflict, grave internal commotion, public calamity, natural disaster, or national, regional, or local emergency, when the President issues an Executive Decree of a State of Emergency; involving the need for the utilization of telecommunications services, the telecommunications providers that operate on public networks are obliged to permit direct control on the part of the head body of the national defense.” See also, Asamblea Nacional Republica del Ecuador, Ley Orgánica de Telecomunicaciones [Telecommunication Law] [http://bit.ly/1Kvdp7W](http://bit.ly/1Kvdp7W).
25 “Entrevista a Alredo Velazco sobre la Nueva Ley de Telecomunicaciones en Ecuador”
26 This event happened outside of the coverage period of the report.
27 Aldo Cassola, Twitter post, June 13, 2015, 7:50 a.m., [https://twitter.com/AldoCassola/status/609734471861114816](https://twitter.com/AldoCassola/status/609734471861114816)
Ecuador

Ecuador is home to three mobile internet service providers: one state-run operator, CNT, and two private providers, Claro and Movistar. Claro holds 62 percent of active cellular accounts, followed by Movistar with approximately 30 percent, and finally, state-run CNT, with less than eight percent of subscribers.\(^{30}\)

There have been no reported incidents of the government placing restrictions on applications from new companies in the ICT sector; however, high registration costs and administrative hurdles can make it difficult to begin operating a new telecommunications business. New ISPs and mobile companies often face fees as high as US$100,000 as well as legal obstacles, both of which can complicate their attempts to enter the market.\(^{31}\)

Regulatory Bodies

In February 2015, Ecuador’s National Assembly passed the Organic Law of Telecommunications. Not to be confused with the similarly named Communications Law passed in 2013, the Organic Law on Telecommunications radically changed the regulation of the telecommunications sector.\(^{32}\)

The new telecommunications law created a regulatory body, the Agency for the Regulation of Telecommunications (Arcotel), which is attached to the Ministry of Telecommunications and is charged with the technical aspects of the administration, regulation, and control of the telecommunications sector and the radio–electric spectrum.\(^{33}\) The previous regulatory bodies—the National Secretary of Telecommunications (Senatel) and the National Council on Radio Broadcasting and Television (Conartel)—were fused together under the structure of Arcotel.\(^{34}\)

The telecommunications law also sets up mechanisms that strengthen the institutional structure and processes of regulation and unification of the regime of telecommunications, including radio and television. The law has drawn criticism, however, for placing Arcotel under the authority of the executive, which may undermine its independence.\(^{35}\)

Limits on Content

*The passage of the 2013 Communications Law granted the government broad authority to censor media for reporting it perceived as biased or inaccurate, a power that has mostly been used to target print and broadcast media. As the government has increasingly curtailed offline media through fines and requests for revisions, new digital ventures and online spaces for political discussion have flourished. In recent years, however, censorship efforts have moved into the online sphere. Facing liability under the Communications Law for third party content, many digital media outlets have closed their comments*

\(^{30}\) ARCOTEL, “Estadísticas: Internet” [Statistics: Internet].


\(^{35}\) “Entrevista a Alfredo Velazco sobre la Nueva Ley de Telecomunicaciones en Ecuador,” http://quintopoder.info/wp/2015/02/13/entrevista-a-alfredo-velazco-ecuador/
Ecuador

section. Although there is no evidence of blocking and filtering, politically motivated copyright complaints have forced the removal of some political content, while evidence suggests that progovernment trolls have skewed national debates. In August 2015, the government declared a state of emergency and ordered prior censorship of all non-government information regarding an active volcano near the capital, a restriction that applied both to traditional media as well as to social media.36

Blocking and Filtering

The government does not engage in systematic blocking or filtering of content in Ecuador. YouTube, Facebook, Twitter, and blog-hosting services are freely available.

Content Removal

As the online public sphere gains prominence as a forum for political discussion in Ecuador, the government has responded by seeking to control online content through a variety of mechanisms, including executive or court orders for content removal, copyright complaints, and coordinated campaigns on the part of government supporters to issue complaints about social media accounts and trigger their suspension.

The restrictive Communications Law, passed in 2013, sparked widespread condemnation from journalists and human rights activists.37 In addition to saddling website owners with “ultimate responsibility” for all hosted content, prescribing arbitrary sanctions on media for unbalanced reporting, and banning “media lynching”—an accusation often applied to investigative reporting in Ecuador38—the Communications Law also grants the media and communications regulator, the Superintendency of Information and Communications (Supercom), the power to audit, intervene, and control all information and media, as well as to enforce regulations governing information and communications.39 Follow-up legislation in 2014 exempted bloggers and social media users from regulation under the Communications Law, but extended the law to cover “all media with an online presence.”40

In practice, Supercom has not aggressively pursued digital media under the Communications Law; however, fines and corrections targeting print media may also affect the online edition of the publication in question. Additionally, the Communications Law holds websites liable for content posted on their sites by third parties. News outlets that have allowed readers to post comments critical of the Correa administration on the comments sections of their websites have faced removal requests, and many newspapers have closed their comments section entirely. Even before the Communications Law, some outlets reported receiving letters from the executive branch demanding that editors or website administrators delete content.41

Reforms to Ecuador’s electoral law in 2012 also have the potential to affect speech. The reform

36 This event happened outside of the coverage period of the report.
39 Martínez, “Ecuador’s Controversial Communications Law In 8 Points.”
banned biased coverage of candidates, which may discourage media outlets from publishing in-depth investigative articles. Under the law, the media is also not allowed to cover the election during the two days before the election begins and on election day itself. Although reports suggest that this law has affected how media organizations reported on the 2013 elections, there is no information about whether the law has resulted in the removal or prior censorship of digital content.42

The Spanish copyright infringement firm Ares Rights has come under fire for its issuance of take-down notices on behalf of the Ecuadorian government. In September 2014, both Facebook and YouTube removed a video called “Lo que Correa no quiere que veas” (“What Correa doesn’t want you to see”), which included images of police repression during student protests that month interposed with statements by President Correa praising the police. YouTube reinstated the video in October after an appeal by the author.43 Most recently, in May 2015, a takedown notice from Ares Rights caused the removal of the YouTube page of the digital rights group Usuarios Digitales (“Digital Users”), although it was quickly restored.44 Ares Rights has issued requests for the removal of more than a dozen photos, videos, and documents that painted the government in an unflattering light.45

In July 2014, activists in Ecuador reported the suspension of four Twitter accounts known to be critical of the government, although it is still unclear what motivated these suspensions or whether they were triggered by legitimate violations of the company’s terms of use.46 In November 2014, the politically active Twitter user Diana Amores denounced Twitter for suspending her account due to a copyright infringement claim issued by Ares Rights. Her account was previously suspended in April 2014 after she retweeted a letter from the president to the people of Quito during local elections in January. On both occasions, Amores’ account was restored after Twitter’s evaluation of the copyright infringement law concluded that it had been used incorrectly.47

Media, Diversity, and Content Manipulation

Although the 2013 Communications Law gives the government broad authority to censor media content, Supercom has almost exclusively used the law to sanction privately-owned traditional media outlets, which are mostly offline. As these sanctions curtail investigative reporting in traditional

media, online media—especially social media, blogging, and reporting by citizen journalists—has actually taken on a greater role in Ecuador’s media landscape.\(^{48}\) In 2014 and 2015, the environment for digital media outlets was much less restricted than that of print and broadcast media. Nevertheless, there are signs that the government is extending its control online through the use of trolls to manipulate content on social media. An order of prior censorship during one national emergency also extended to regular social media users, potentially restricting free expression about an important national concern.

Although there is no clear case of the government using the Communications Law to target digital media publications or to target exclusively online content, the government’s broader restrictions on traditional media outlets likely affect digital content associated with these outlets both by encouraging self-censorship and by restricting financial resources for independent media. For example, although offline material has been the primary target of sanctions in the past, newspapers seeking to avoid sanctions may avoid publishing controversial articles in both the offline and online editions of their newspapers.

Under the Communications Law, the regulator has fined newspapers for content that was critical of the government and has even meted out fines to media outlets for failing to cover events that might generate positive publicity.\(^{49}\) In the two years that the Communications Law has been in effect, Supercom has issued 313 resolutions, affecting 198 media outlets and resulting in 185 financial sanctions against outlets.\(^{50}\) Another study of Supercom rulings found that only one public media outlet has ever been sanctioned.\(^{51}\) Fines on newspapers for violations of the Communications Law, and the associated legal battles, may sap resources from independent media outlets. This economic impact on private media may be exacerbated by the fact that some companies appear reluctant to advertise in media that is critical of the government.\(^{52}\)

In early 2014 the popular humorist Xavier Bonilla (known as Bonil) published a cartoon in both the print and online editions of the newspaper *El Universo* satirizing the police raid on the home of Francisco Villavicencio. The cartoon, which went viral, was posted and retweeted on social media thousands of times before Bonil and *El Universo* were charged with violating provisions of the 2013 Communications Law.\(^{53}\) Bonil was also ordered to issue a formal correction of his cartoon, and *El Universo* was fined two percent of its earnings for the three months prior to the verdict.\(^{54}\) As of May 2015 the defense appeal is still pending; however, in the corrected version of his cartoon, which was meant to portray only the facts as reported by the authorities, Bonil once again managed to criticize

---

48 Examples of new blogs include: estadodepropaganda.com, insulabarataria.wordpress.com, and sentidocomun.com.
50 Teresa Mioli, “Sancciones contra medios independientes continúan en Ecuador luego de dos años de la Supercom,” [Sanctions against independent media continue in Ecuador after two years of Supercom], *Blog Periodismo en las Américas*, Knight Center at The University of Texas Austin, July 6, 2015, [http://bit.ly/1LOK0YL](http://bit.ly/1LOK0YL).
52 John Otis, “Ecuador’s year-old media law stifles in-depth reporting,” The Committee to Protect Journalists (blog), June 24, 2014, [http://cpj.org/x/5ba8](http://cpj.org/x/5ba8).
Ecuador

the government with an overly polite rendition of the raid that made light of the request to formally correct his cartoon.\(^{55}\)

In February 2015, Bonil was sanctioned and ordered to correct his work a second time under the Communications Law after he published a cartoon mocking a congressman, which the regulator deemed to be discriminatory.\(^{56}\) Apparently, however, the sanction did not lead to removal of the online content: as of May 2015, it was possible to see the originals of both sanctioned cartoons on *El Universo’s* website, as well as the correction of the cartoon satirizing the raid on Villavicencio.\(^{57}\)

Although the Communications Law exempts social media users from sanctions, the government has begun censoring social media users through other means. In one particularly concerning case, the government completely prohibited discussion about a national emergency, not only for the media but also for individual social media users. On August 15, 2015, President Correa signed a decree declaring a state of emergency when a volcano, Cotopaxi, located 50 km south of Quito, began spewing ash after 73 years of inactivity. In the decree, the government prohibited the media and social media users from discussing the volcano in order to “avoid rumors and disinformation.”\(^{58}\) Free speech organizations roundly condemned this action for undermining the role of the media in protecting people from disaster, disseminating information, and holding the government accountable for its response.

Legislation introduced to Ecuador’s National Assembly in June 2014 would create a constitutional amendment to classify communications as a public service. Although the 2013 Communications Law already has a similar provision, a constitutional amendment would cement and strengthen this principle. Free speech advocates worry that the amendment, which was still under debate as of May 2015, would erode free speech, as the government might expand the use its regulatory powers to determine content.\(^{59}\)

Social media is extremely politicized in Ecuador, and the government has regularly encouraged social media users to attack individuals who insult, threaten, or criticize the government. The most notable case occurred in January 2015 when President Correa criticized three social media users in his weekly presidential address.\(^{60}\) Shortly after the president called out critics, the government announced the creation of a website, Somos Mas (“We Are More”). According to a government news bulletin, the purpose of Somos Mas is to connect followers to “government campaigns aimed at democratizing access to media and ending abuses on social media” and “to create a front against attacks from people, who hiding in anonymity, are always present in virtual spaces.”\(^{61}\) Critics argued that this website would encourage followers to reveal private information about anonymous social media users and would unleash thousands of trolls to harass government critics.\(^{62}\) Although the

---

59 John Otis, “How Ecuador’s plans to make communications a public service is threat to free press,” Committee to Protect Journalists (blog), January 20, 2015, [http://cpi.org/v/5eaf](http://cpi.org/v/5eaf).
60 AP, “Ecuador President’s Social Media Counter Attack,” *New York Times*, February 2, 2015, [http://nyti.ms/1VSMFir](http://nyti.ms/1VSMFir).
Ecuador

Somos Mas initiative ultimately failed to catch on and gather the army of hoped-for supporters, the direct involvement of the executive in implicitly encouraging harassment and attacks on anonymity is concerning.63

The Ecuadorian government has also been accused of manipulating conversations online via pro-government commentators, reportedly employed to counter opposition voices. In 2012, a series of interviews with government insiders and investigative journals pointed to the existence of a digital army slandering and discrediting dissidents online.64 Unconfirmed reports in 2015 also detailed the existence of online users employed to monitor and respond to opposition social media with pro-government propaganda.65

The new telecommunications law, passed in February 2015, protects net neutrality in principle and states that access providers cannot “restrict, block, interfere, discriminate, hinder, prioritize, or restrict the rights of their users or subscribers to use, send, receive or offer any content, application, development or legal service through the internet.” Civil society groups, however, have raised concerns that these protections are weakened by other provisions in the law which providers may be able to exploit as loopholes to net neutrality.66 In April 2015, the Ministry of Telecommunications ruled that mobile internet providers could not limit calls on WhatsApp, after several mobile providers had proposed limiting this service in certain plans. The Ministry cited the new telecommunications law’s protections of net neutrality as the basis for its ruling.67

Digital Activism

During late-2014 and early-2015, a controversial constitutional revision and financial shortages triggered protests and social movements across Ecuador.68 By summer of 2015, protests over these issues, as well as proposed tax increases, gathered steam, and a series of mobilizations brought thousands of people into the streets.69 Social media has taken on a central role in activism and citizen reporting in the context of these demonstrations.70 Earlier in the year, social media users and internet freedom organizations also rallied to defend social media users targeted by the president and government supporters.

President Correa’s targeted attacks on the Facebook page Crudo Ecuador galvanized many people to defend it and internet freedom more broadly (see Intimidation and Violence). After the president appeared to encourage followers to “dox” anonymous online critics, exposing their identifying in-
Ecuador

formation to facilitate harassment, several internet freedom organizations drafted and signed the Manifesto for the Freedom of Expression, Anonymity, and Online Privacy in Ecuador, a defense of the decentralized internet and online anonymity.\footnote{Agencia de Noticias Medio a Medio. “Ecuador: Usuarios digitales pronuncian por la libertad de la expresión en internet,” February 5, 2015, \url{http://bit.ly/1G7Ct5S}.}

Internet and digital rights organizations celebrated a partial victory after the new penal code went into effect in August 2014. Although it contains several concerning provisions (see Legal Environment), the code went into effect without some of the most controversial anti-privacy provisions as a result of digital activism. In 2013, the internet activist organizations Usuarios Digitales (“Digital Users”), Apertura Radical (“Radical Openness”), and Asociación de Software Libre del Ecuador (“Ecuador Association of Free Software”) launched a campaign on social media under the hashtag \#InternetLibre to lobby against the proposed surveillance provisions in Article 474 of the proposed penal code.\footnote{Usuarios Digitales, Campaign launched on Facebook: \url{https://www.facebook.com/InternetEcuador}; See also: GKillCity.com, “Free Internet,” November 18, 2013, \url{http://gkillcity.com/dossier/internet-libre}.} Had the new penal code been approved with Article 474 intact, ISPs would have been forced to record all user activity—including IP addresses—for six months, and cybercafes would also have been required to install surveillance equipment in order to record video footage of customers.\footnote{Juan Arellano, “Ecuadorean Activists Say No to Cybercafe Surveillance,” trans. Victoria Robertson, \textit{Global Voices Advocacy}, November 19, 2013, \url{http://bit.ly/1LONtN1}.} Due in large part to civil society action, legislators removed Article 474 before the new penal code was passed in November 2013.\footnote{“[2013 Assessment] Privacy and Surveillance in Ecuador,” trans. Amalia Toledo, \textit{Digital Rights LAC}, January 28, 2014, \url{http://bit.ly/1WdEcq}.}

Despite a mixed record on internet freedom, the Ecuadorian government has created some promising initiatives to promote open government and online citizen participation on issues related to internet freedom and privacy. In February 2014, for example, the National Secretary for Higher Education, Innovation and Technology launched the region’s first wiki legislation project (WikiCOESC+i). This freely accessible site allowed citizens of Ecuador and other nations to propose changes to the Organic Code for Social Economy of Knowledge and Innovation, with the goal of designing a framework for the “inclusive and democratic” development of an open knowledge society.\footnote{Secretaria de Educación Superior, Ciencia, Tecnología e Innovación, Código Orgánico de Economía Social del Conocimiento e Innovación [Organic Code for Social Economy of Knowledge and Innovation] accessed April 21, 2014, \url{http://bit.ly/1mip29X}.} More than 16,000 users participated in the creation of this legal code, which underwent more than 40,000 text edits. In June 2015, the resulting Innovation Code, which classifies internet as a basic service and significantly reforms Ecuador’s intellectual property regulation, was presented to the legislative assembly for debate.\footnote{This event occurred after the formal coverage period for this report. “Código INGENIOS llega al Legislativo para cambiar ‘la historia’ y fomentar el conocimiento en Ecuador,”[Innovation Code arrives in the legislature to change ‘history’ and spur knowledge in Ecuador], Public Agency of News from Ecuador and South America, June 4, 2015, \url{http://bit.ly/1VSICVZ}; See also Andrés Jaramillo, “Código Orgánico de la Economía del Conocimiento ecuatoriano será presentado en la Asamblea,” [Organic Code of the Knowledge Economy will be presented in the Assembly] \textit{El Comercio}, May 24, 2015, \url{http://bit.ly/1NOOqms}.}

\section*{Violations of User Rights}

\textit{Although prosecutions and physical attacks against online users are rare in Ecuador, some users have faced harassment and threats, government surveillance, and technical attacks. In 2015, President Correa targeted critical social media users in his televised presidential address, encouraging followers}
Ecuador

to dox anonymous users. The president’s statements contributed to an environment of harassment, in which multiple social media users faced online and offline threats. In August 2014, the new penal code entered into force. Although the penal code eliminates some charges for defamation, it retains several provisions that limit freedom of expression.

Legal Environment

Ecuador’s constitution guarantees “universal access to information technologies and communication” (Article 16.2), and confers the ability to exercise one’s right to communication, information, and freedom of expression (Article 384).77 The country, however, faces several threats to free expression, including criminal provisions against libel, government regulation and oversight of media content, and concerns about judicial independence.78

In August 2014, the new penal code entered into force. Although it eliminates criminal charges for insult, it retains criminal charges for slander and libel, as well as restrictions on social protests and privacy protections that some critics worry may limit investigative reporting and whistleblowing.79 Article 179 establishes a prison sentence of six months to a year for any person “who, by virtue of his/her state or office, employment, profession, or art, has knowledge of a secret whose divulgement might cause harm to another and reveals it.” The article makes no exception for revealing information for the public interest. Article 229 places further restrictions on divulging information by banning the revelation of registered information, databases, or archives through electronic systems in a way that violates the intimacy or privacy of someone else. Again, there is no exception in this article for whistleblowers or journalists. Article 307 establishes a penalty of five to seven years in prison for creating economic panic by “publishing, spreading, or divulging false news that cause harm to the national economy in order to alter the prices of goods.”80

The 2013 Communications Law grants a government media oversight committee the power to regulate media and issue civil and criminal penalties to journalists or media outlets who fail to report in a manner that the regulator deems fair and accurate. Although the law has not been used to target or fine exclusively digital media outlets, Article 3 of the law expands the regulator’s control to “all media with an online presence.” The vague language in the law raises concerns that it will be used to target online media in the future (see Content Removal and Media, Diversity, and Online Content Manipulation).

Prosecutions and Detentions for Online Activities

There were no known cases of journalists or online users being jailed or detained for online speech. One isolated instance of a user being sentenced in a civil court to 15 to 30 days of jail time for online defamation was quickly dismissed upon appeal. Nevertheless, the legal harassment of offline journalists with charges of criminal libel and other charges under the 2013 Communications Law raises concerns that in the future these laws will be expanded to prosecute online reporters.81

---

81 Fundamedios, “Escandidata denuncia a dos medios ante la Supercom y demanda penalmente a uno de sus directivos,” [in
In October 2014, the Civil Court in the city of Sucúa sentenced the former city councilor, Jaqueline González, to fifteen days in prison for allegedly posting a Facebook comment that denounced a land conflict, implicating an indigenous leader and a lawyer in the land invasion. González denied that the Facebook account, which was under the name Jakelin Gonzalez, even belonged to her. Despite this contention, she was found guilty under Article 396 of the Penal Code, which prohibits the proffering of expressions that “discredit or dishonor” someone else under penalty of a 15 to 30 day prison sentence. Upon second appeal, González was declared innocent, and she never served jail time.

Online writers have also incurred high penalties in civil libel cases. When online blogger Miguel Palacios Frugone sued President Correa for libel after the president called him a “rapist,” President Correa responded in kind by countersuing Palacios for defamation over twenty articles that he produced on his blog Desde mi Trinchera (“From my Trench”) criticizing the president. On July 22, 2015, the National Court of Justice ruled in President Correa’s favor and ordered Palacios to pay a fine of US$46,000 for “moral damage” incurred by at least two of his online posts.

Several individuals have been arrested on charges that they hacked the personal Twitter or email accounts of President Correa. In May 2014, the government detained two teenage boys on charges of hacking the president’s Twitter account; however, they were released the following morning due to lack of evidence. In December 2013, President Correa announced that his email had been intercepted by representative Cléver Jiménez and online journalist Fernando Villavicencio—both of whom already faced libel charges from a report they wrote asking the Attorney General to investigate the president’s role in ordering an armed intervention in a hospital during protests that year. After raids on their offices, they were accused of high-level espionage, although they were never charged. As of June 2015, the investigation into the espionage case was still open.

In January 2014, the court sentenced Jiménez and Villavicencio to eighteen months in prison for libel, and both individuals went into hiding. In March 2015, however, the court dismissed charges, in light of the numerous delays in judicial process and changes in the penal code eliminating criminal libel. Carlos Figueroa, a doctor and activist involved in the same case, was also charged and had already completed a sentence of six months in prison by the time the court reevaluated the case.

Although the libel charges pertained to an offline report, the free speech organization Fundamedios has raised the possibility that Villavicencio was targeted partially in retaliation for writing about corruption for the online publication Plan V.

83 Interview with expert at Fundamedios, July 31, 2015.
88 Soraya Constanza, “Los condenados por injuriar a Correa ya no tienen que esconderse.”
Surveillance, Privacy, and Anonymity

Little information is available about the extent of surveillance in Ecuador; however, the current legal structure provides little protection from the government collection of metadata. Civil society groups have repeatedly raised concerns about the country’s investments in advanced surveillance technology; most recently, these concerns have centered on the Ecuadorian government’s contracts with the Italian technology company Hacking Team. Anonymity also came under attack during the coverage period. Although neither anonymous nor encrypted communications are prohibited in Ecuador, in January 2015 the government encouraged followers to dox anonymous social media users who were critical of the government. The internet rights advocacy organization Usuarios Digitales strongly condemned this action as a violation of users’ right to anonymity on the internet.90

After the security breach at the Italian information technology company Hacking Team on July 6, 2015, several sites, including WikiLeaks, published the company’s leaked email exchanges.91 The revelations triggered a major scandal worldwide because many of the company’s clients were governments with a history of human rights violations. In Latin America, Ecuador appeared as one of their major customers, third only to Mexico and Chile. Although Ecuador’s intelligence agency denied having contracts with Hacking Team,92 evidence from leaked emails suggests that not only did the government have contracts with the company for surveillance technology, it may have used this technology to target opposition figures or activists with malware.93 The Ecuadorian intelligence agency SENAIN sent several requests to a Hacking Team customer support engineer for assistance in sending spyware to email and phone accounts that appear to be linked to Carlos Figueroa, an opposition activist. At the time, Figueroa was in hiding from the government after being charged with libel, in what many regarded as a politically motivated case. Leaked emails also suggest that the government used Hacking Team tools to develop documents booby-trapped with malware, giving them titles that reference the Yasuni wilderness reserve. Critics have raised concerns that these documents may have been created to ensnare environmental or indigenous activists who are involved in protests against government plans to drill for oil in the reserve. In the wake of the revelations, several journals and online magazines suffered distributed denial-of-service (DDoS) attacks after publishing information regarding the leaks.94

The Hacking Team revelations have sparked a major debate in traditional media outlets and on social media.95 In the weeks after the leak, media activists and house representatives protested outside the offices of Senain (National Intelligence Office) located in the suburbs of Quito,96 and protests against the government, already widespread in the summer of 2015, began to incorporate demands for transparency over surveillance of citizens.

Beyond the Hacking Team leaks, there is some evidence that the Ecuadorian government has also

---

93 AP, “Correction: Ecuador-Hacking The Opposition Story;”
95 Interviews on the Channel 1 editorial journal with Andrés Carrion: “En la Polémica – Hacking Team y SENAIN,” YouTube video, 58:05, published by Aldo Cassola, July 20, 2015, https://www.youtube.com/watch?v= hC4r2mFX0
Ecuador

Although invested in the purchase of other surveillance systems. The Russian company Speech Technology Center alleged in international media reports that Ecuador installed the world’s first biometric surveillance system with voice and facial identification capabilities. Authorities can use this software to build up a library of voiceprints of criminals or other individuals and then use it to identify individuals in intercepted calls.\(^97\) Documents have also surfaced detailing government attempts to purchase surveillance drones from overseas contractors.\(^98\) The government has defended its right to conduct surveillance in criminal investigations, but has said that it does not engage in such activities for political purposes.\(^99\) To date, the administration has neither confirmed nor denied reports of the installation of a biometric surveillance system or of attempts to purchase drones for surveillance.\(^100\)

Ecuador’s legal framework provides the government with broad authority to request user information without judicial oversight. The 2015 Organic Law on Telecommunications guarantees user privacy and requires service providers to notify users in the case of third party interception of communications. Despite such positive provisions, however, Article 84 says that service providers must give authorities access to data for the purpose of investigating crimes.\(^101\) The article says that Arcotel will establish the necessary provisions for access to this data at a future date, but it is not clear that the law will require a judicial order for access to data. This is consistent with previous telecommunications regulations. In 2012, the Telecommunication Service Subscribers and Added Value Regulation Resolution authorized the telecommunications regulator to track IP addresses from ISP customers without a judicial order.\(^102\) In 2013, civil society successfully blocked a government initiative that would have required ISPs to record and store all user data for six months and would have forced cybercafes to record video footage of customers.\(^103\)

Although cybercafes do not have to film users, the government requires that cybercafe users register with the Ministry of Telecommunications with their full name, phone number, passport number, voting certificate number, email address, and home address. Users must also agree to terms that stipulate that all information entered into the database during use falls under the jurisdiction of the telecommunications regulator.\(^104\) If a user infringes on the terms and criminal charges are applicable to the transgression, the user will be prosecuted under Ecuador’s penal code.

**Intimidation and Violence**

Although levels of harassment and violent threats against journalists did not reach the same levels in

---


\(^99\) Rosie Gray and Adrian Carrasquillo, “Ecuador Defends Domestic Surveillance,” *Buzzfeed*, June 27, 2013, [http://bzfd.it/1QT1K4U](http://bzfd.it/1QT1K4U).


\(^102\) See Article 29.9; [http://bit.ly/1GPH0aE](http://bit.ly/1GPH0aE).


\(^104\) The terms of the agreement refer to Senatel and the superintendence of telecommunications, Supertel. Although these two bodies have been subsumed under Arcotel, the new telecommunications authority established in 2015, the online form used to register cybercafes has yet to change the previous language to indicate this. SENATEL, “Registro de CibercafesOn Line” [Registration of Cybercafes Online], accessed August 6, 2013, [http://bit.ly/1WdJf6P](http://bit.ly/1WdJf6P).
Ecuador

Ecuador as in other countries in the region, the direct involvement of the president in inciting social media battles, with little concern about the harassment and violence that could result, represents a worrisome development. During the coverage period, social media competition between pro-government supporters and the opposition escalated, with both government supports and critics issuing threats against one another, and with at least one individual receiving death threats at his home after the president repeatedly called for social media users to criticize him.

In his weekly televised presidential address in January 2015, President Rafael Correa identified social media accounts that had used Twitter or Facebook to criticize or insult him and called for his followers to criticize these users online. Among the accounts called out by the president was the popular Facebook page Crudo Ecuador, which had recently published a meme juxtaposing an image of the President Correa shopping in an upscale European mall with a declaration the president had made that online shoppers should be taxed for buying goods from overseas. At the time, the administrator of Crudo Ecuador was anonymous, which the president used as ammunition for a broader attack on online anonymity. During his address, Correa said “we are also going to identify these people to see if they are so humorous when the whole world knows who they are...If they send one tweet, we will send 10,000.” The following week, President Correa announced the creation of Somos Mas, a website where people could share information about social media users who were criticizing the government. Critics alleged that Correa was marshalling his followers for the express purpose of harassing social media users.

Shortly after the television announcement, Twitter users doxed the administrator of Crudo Ecuador, Gabriel González, revealing his name, his address, his ID number, the names of his family members, and a cell phone picture of him taken at a mall. González said that some of this information came from confidential documents he filed to register the Crudo Ecuador brand with the Ecuadorian Institute of Intellectual Property. On February 19, 2015, González shut down the Twitter account of Crudo Ecuador and stopped posting on the Facebook page, announcing the shutdown with the hashtag #UstedGanó (“You Won”) and citing harassment and threats as the motive. González also posted a picture of a bouquet of flowers with a threatening note that he had received while on vacation with his family.

Although the president’s campaign against Crudo Ecuador and other Twitter users gained more attention in the international media than previous campaigns, it was not the first time that the pres-

---

105 Abuse of social media users from pro-government supporters is well-documented, but it appears that in the environment of a highly polarized social media war, government critics have also leveled threats and attacks against normal social media users. The Twitter account Anonymous Ecuador has begun identifying pro-government supporters and encouraging its followers to “send a greeting to this Correa supporter,” often unleashing a flurry of criticisms as well as violent attacks. For example: Nueva Fuerza Rural, Facebook post, August 20, 2015, http://on.fb.me/1LrFnpt.
107 Manuel Rueda, “Ecuador’s president declares a war on memes,” Fusion, January 22, 2015, http://fus.in/1EphhIO.
109 The website can be accessed at www.somosmas.ec.
112 The issue was widely publicized after it was covered in the HBO Show Last Week Tonight with John Oliver. Last Week Tonight with John Oliver, “Ecuador’s Sensitive President,” YouTube video, 4:11, February 9, 2015, https://www.youtube.com/
Ecuador

ident has marshalled his Twitter followers to insult critics. On March 29, 2014, President Correa disparaged the journalist Betty Escobar—who had criticized his trip to the United States in a column in the newspaper El Universo—calling her a “hater” and a “coward” in his weekly televised address and telling viewers to “check out” her Twitter username. On April 7, 2014, in a threat closely resembling the one later sent to Crudo Ecuador, anonymous individuals sent a threatening note and flowers to Escobar in New York and to her family in Guayaquil Ecuador.113 In a televised speech in February 2014, Correa called on his Twitter followers to insult the cartoonist Bonil after he drew a cartoon critical of the government.114

Further incidents in 2014 and 2015 revealed harassment and threats that appeared after journalists criticized public officials or the police. On May 17, 2015, Andrés Mendoza, a journalist with the Agen-cia Popular de Comunicación Ser Públicos, received a threat stating that he would be killed within 72 hours if he did not remove videos he had posted showing forced evictions in Guayaquil and police abuses during the seizure of the Ecuadorian Teacher’s Unemployment Fund. The threat arrived to his personal Facebook account and the email account of Agencia Popular. Three days later, Mendoza received an email referencing his funeral.115 In November 2014, unknown individuals entered the offices of the digital and print media organization Cotopaxi Noticias and stole six computers.116 In January 2014, political activist, filmmaker, and writer Carlos Andrés Vera, who owns the popular blog Polificción, was targeted on Twitter. After his 3-year-old son was threatened, reportedly by a government representative, Vera announced that he would be abandoning online activism and would be removing himself from online political debate.117 There has also been at least one report of an individual dismissed from his work as the result of commentary he made on Twitter.118

Technical Attacks

Accusations of data manipulation, hacking, and other forms of cyberattacks have been leveled from both government and opposition groups during recent years. While such attacks—which have included modifications to webpages (defacements), phishing, and the spread of malware—have been sporadic rather than systematic, they appear to be on the rise. On July 7-8, 2015, at least three online news outlets reported DDoS attacks after reporting on contracts that the Ecuadorian government had with the Italian information technology company Hacking Team (see Surveillance, Privacy, and Anonymity).119

watch?v=nMdDykp_KXs
114 John Otis, “Pressed by government, Ecuadoran cartoonist is forced to adjust,” Committee to Protect Journalists (blog), July 8, 2014, http://cpj.org/x/5be5.
118 This event occurred outside the coverage period. See: Martín Pallares es despedido de El Comercio por sus comentarios enfrentes a Correa’s “incompetence.”
119 This event occurred outside the coverage period and therefore had no impact on scores. Samuel Woolley, “#HackingTeam Leaks: Ecuador is Spending Millions on Malware, Pro-Government Trolls,” Global Voices, August 4, 2015, http://bit.ly/11Us6z.
Ecuador

The websites of advocacy groups and news media organizations have occasionally been subject to DDoS attacks and unexplained disruptions. On February 9, 2015, the free speech organization Fundamedios announced that their website suffered a DDoS attack and was down for a day. The DDoS attack occurred a few hours after the release of the organization’s 2014 report on freedom of speech violations in Ecuador. In the same month, hackers attacked the webpage of the newspaper La Hora, causing the site to crash for a day.

In 2014 and 2015, government websites as well as the personal email and Twitter accounts of government officials were subject to cyberattacks from individuals who identified with Anonymous and other groups. In March 2014, Anonymous hacked the president’s Twitter account, which it used to tweet allegations of corruption against a high-level official from the Ministers of Interior and the Intelligence. Despite the security breach, the account was restored after a few hours.

121 Fundamedios, “Página web de Fundamedios es víctima de ataque cibernético.”
Key Developments: June 2014 – May 2015

- Self-censorship has risen among online journalists and social media users alike (see Media, Diversity, and Content Manipulation).

- Cybercrime and antiterrorism laws were proposed over the coverage period, criminalizing several broad online offenses and sparking fears that the laws could be used to crack down on human rights activists and government critics. The antiterrorism law was enacted in August 2015 (see Legal Environment).

- Two online journalists were sentenced to life imprisonment in April 2015. Abdullah al-Fakharany and Samhi Mustafa, respectively the executive director and cofounder of the news website Rassd, had been in detention since the dispersal of a pro-Mohamed Morsi sit-in in August 2013 (see Prosecutions and Detentions for Online Activities).

- At least two users were handed prison sentences for insulting religion online, and LGBT users faced arrests for YouTube videos under the crime of “inciting debauchery” (see Prosecutions and Detentions for Online Activities).

- Extralegal attacks by angry mobs for religious speech—sometimes with the complicity of local security forces—remains a security concern for ordinary users. In May 2015, 18 members of 5 Christian families were expelled from their homes after one man allegedly published a Facebook post insulting the prophet Mohamed (see Intimidation and Violence).
Introduction

The internet is increasingly seen as a “security threat” in Egypt, including by newly elected president Abdel Fattah el-Sisi. Internet penetration has improved very slowly in the country, which has been plagued by political uncertainty and economic strife since the 2011 revolution that ousted longtime president Hosni Mubarak. Space for political opposition has dwindled both under former Islamist president Mohamed Morsi, as well as under President el-Sisi, who as defense minister and head of the armed forces removed Morsi from power in June 2013. A new constitution was passed by referendum in January 2014, and presidential elections that May brought el-Sisi to power with over 90 percent of votes. Since then, he has been ruling by decree, given that there is currently no parliament.

Despite the existence of nominal guarantees in the constitution, the legal environment has tightened following the 2013 coup. Restrictions on freedom of assembly were passed in November 2013, and in September 2014, a new law made it a potentially capital offence to accept funding from foreign countries in order to commit an act “harmful to the national interest, or compromising the country’s sovereignty,” a broad term that activists and journalists worried could apply to critical reporting or online campaigns against human rights abuses. Nongovernmental organizations (NGOs) also face increasing pressure under strict laws requiring them to register with the authorities and obtaining approval for receiving foreign funding. In addition, new cybercrime and antiterrorism laws were proposed that included harsh penalties for broadly worded crimes applicable to online activities, such as setting up websites that could be construed as being related to terrorism. The antiterrorism law was passed in August 2015, despite fervent criticism from local activists and the international human rights NGOs.

Journalists and social media users continue to be prosecuted for political, social, and religious speech. In April 2015, Abdullah al-Fakharany and Samhi Mustafa, respectively the executive director and co-founder of the news site Rassd, were sentenced to life in prison for their coverage of the violent dispersal of a pro-Mohamed Morsi sit-in in August 2013. They were detained during that month for “disturbing the peace,” but a judge later increased the charges to “spreading chaos,” “spreading false information,” and “forming an operations room to direct the Muslim Brotherhood to defy the government.” At least two users were handed prison sentences for insulting religion online, and LGBT users faced arrests for YouTube videos under the crime of “inciting debauchery.”

Meanwhile, extralegal attacks by angry mobs for religious speech—sometimes with the complicity of local security forces—remains a security concern for ordinary users. In May 2015, 18 members of 5 Christian families were expelled from their homes after one man allegedly published a Facebook post insulting the prophet Mohamed. Finally, confirmation that the government possesses surveil-

lance malware and the establishment of the “High Council for Cybersecurity” has led to increasing concerns over the government’s security-centered approach to regulating the internet, which flouts human rights standards and is setting the stage for more restrictions on internet freedom in advance of parliamentary elections slated for the end of 2015.

**Obstacles to Access**

*Poor telecommunications infrastructure, frequent power blackouts, and relatively high costs continue to pose obstacles to universal internet access in Egypt. The government’s control over the internet backbone and the dominant ISP dampens market competition and allows the authorities to shut down networks during sensitive political events.*

**Availability and Ease of Access**

The development of Egypt’s information and communications technology (ICT) sector has been a strategic priority since 1999, when former president Hosni Mubarak created the Ministry of Communications and Information Technology (MCIT) to lead Egypt’s transition into the information age. Since then, ICT use has increased rapidly, with internet penetration growing from 20 percent in 2009 to 32 percent by the end of 2014, according to figures from the International Telecommunication Union. Mobile internet users via mobile phones or USB modems accounted for roughly 46 percent of all internet use, with ADSL use at around 34 percent. Egypt’s mobile phone penetration rate was 111 percent in January 2015, amounting to over 95 million mobile subscriptions. Although these figures are promising, there are a number of obstacles hindering access to ICTs, including an adult literacy rate of only 74 percent, poor telecommunications infrastructure in rural areas and urban slums, and flagging economic conditions.

Broadband, though cheaper than in some neighboring countries, is more expensive thanks to a dominant state-owned internet provider. An unlimited 1 Mbps connection costs US$20 (EGP 140) per month, whereas in Morocco, for instance, a 4 Mbps connection costs US$12. Moreover, most providers implement a cap on high-speed internet, under what has been marketed since 2007 as a “fair use policy.” The fair use policy has been implemented even on supposedly unlimited connections, causing speeds to slow drastically.

Furthermore, the overall poverty of Egyptian households impedes access to broadband internet. Telephone lines are not universal, with large segments of the country unconnected to the landline telephone grid. Even when they are, the phone infrastructure, based on antiquated underground copper lines, frequently does not allow for speeds above 1 Mbps. In the ITU’s ICT Development In-

---

Egypt

dex, a composite index which compares developments in ICT across countries, Egypt ranked 89th out of 166 countries in 2013, two steps back from the previous year.13

Restrictions on Connectivity

The Egyptian government has centralized internet infrastructure and fiber-optic cables into highly controllable “chokepoints.”14 In addition, virtually all of Egypt’s telecommunications infrastructure is owned by Telecom Egypt, a state-owned company. The arrangement makes it easy to suspend internet access or decrease speeds, as was the case during the 2011 revolution. From January 27 to February 2, 2011,15 authorities disabled the country’s Border Gateway Protocol Routes, shutting down all internet traffic in less than one hour.16 Telecommunications companies were then ordered to cut mobile internet and text-messaging services under the terms of strict agreements they had signed with regulators. At the time, state intelligence agencies claimed that “foreign intelligence [was] using communication technologies to plan terrorist actions.”17

ICT Market

The Egyptian mobile phone market is divided between three companies. Mobinil, founded by construction magnate Naguib Sawiris, is now 99-percent owned by the French company Orange. The company had over 33 million subscribers by end of 2014. Vodafone Egypt, around 55 percent of which is owned by Vodafone, had over 39 million subscribers. Finally, Etisalat Misr, of which the UAE company Etisalat (UAE) owns 66 percent, had 22 million subscribers.18 The state-owned company, Telecom Egypt, obtained a license for a new mobile telephone company in April 2014 but has yet to launch service. In the fixed-broadband market, Telecom Egypt (under the banner TE Data) controls 63 percent of the ADSL market.19 Egypt’s main ISPs, also known as Class A ISPs (Etisalat Egypt, LINKdotNET, Vodafone data) lease lines from TE Data and resell bandwidth to over 200 smaller ISPs.

Regulatory Bodies

Mobile service providers and ISPs are regulated by the National Telecommunications Regulatory Authority (NTRA) and governed by the 2003 Telecommunication Regulation Law. The NTRA’s board is chaired by the ICT minister and includes representatives from the defense, finance, and interior ministries; the state security council; the presidency; workers’ unions; as well as public figures, experts, and other military figures.20 Officially, the NTRA is responsible for regulating the telecommunications industry21 and furthering ICT development through projects like the “eMISR” National Broadband

---

Plan outlined in late 2011. The NTRA also conducts analysis of the telecommunication market and publishes research to encourage investment. However, there have been some reports revealing the NTRA's ties to online control and surveillance activities. Through its control of the mobile subscriber database, it has been accused of monitoring mobile and social media applications.

**Limits on Content**

Authorities in Egypt do not engage in blocking or filtering of online content, and news sites are rarely contacted by the government to remove content. Access to social media is freely available and the use of services such as Facebook, Twitter, and YouTube remains widespread. However, self-censorship is increasingly pervasive, even among online journalists. Political turmoil in the country has created a highly polarized environment in which individuals are less comfortable expressing their opinions online. Recent laws criminalizing online activities and heavy jail sentences against online journalists affiliated with the Muslim Brotherhood have had a chilling effect on independent reporting and digital activism.

**Blocking and Filtering**

Egypt does not block access to political, social, or religious content online. YouTube, Facebook, Twitter and blog-hosting services are freely available. Lawsuits to ban pornography or social media platforms have taken place over the past years, with mixed success. In March 2015, during the government-organized “Egypt Economic Development Conference” (EEDC) in Sharm el Sheikh, the website of Human Rights Watch was reportedly blocked within the conference premises. Access was reestablished after a journalist tweeted about it.

A new cybercrime bill, approved by the Council of Ministers in April 2015 and awaiting the president's signature as of October 2015, would create new legal requirements for internet service providers. Under article 19, the police and public prosecutor would be able to submit a request to block websites containing “quotes numbers, photos, videos, and any other material” deemed a threat to national security. A court would have to rule on the request within 24 hours. Police may also bypass the court order in “cases of emergency.” Internet providers refusing to implement a blocking ruling will be punished by a jail sentence of no less than three years and a fine ranging from USD 80,000 to USD 160,000; however if that refusal to block a website leads to “the death of one or more persons, or damage to national security,” the sentence will be life imprisonment and a fine of USD 450,000 to USD 3 million.

Egyptian courts have consistently ruled to ban pornographic websites. Rulings by administrative
Courts in 2015 and 2009 were not implemented; a separate court case from 2013 decided against a ban on online pornography.\(^{29}\) Previously, the ban was estimated to cost as much as EGP 100 million (USD 14 million),\(^{30}\) with a significant effect on internet speeds. Civil society organizations have objected to the threat of a ban, both on grounds of freedom of expression but also because of the high expense. Nevertheless, several ISPs have implemented the court’s decision on a voluntarily basis, offering a “safe internet service” to subscribers.

In May 2014, a lawyer pressed charges against the prime minister and the minister of telecommunications to demand that Facebook be banned, arguing that the website is used to spread immorality, rumors, and falsified news detrimental to the state. Given how easy it is to create an account, the lawsuit adds, it is possible to create pages falsely representing state agencies, such as Egypt’s General Intelligence and the Supreme Council for Armed Forces, or public officials. In response, the State Litigation Authority stated that blocking Facebook would impede on citizens’ constitutional rights, pointing that millions use the website to share photos and express their opinions. It also added that even Saudi Arabia has not blocked the website. A ruling was due for mid-2015.\(^{31}\)

Voice over Internet Protocol (VoIP) services are not restricted, even though it is technically prohibited to make international calls from mobile networks under Article 72 of the Telecommunications Law, which forbids the “by-passing [of] international telephone calls by any means whatsoever.”\(^{32}\) Thus, VoIP calls through services such as Skype and Viber can only officially be placed over fixed-line or Wi-Fi networks, not through 3G.\(^{33}\) The debate over VoIP flared up in June 2013 after the National Telecommunications Regulatory Authority (NTRA) announced the establishment of a committee to “monitor” communications on free messaging apps WhatsApp and Viber, pending a potential decision to block or restrict them. The NTRA’s declaration said that the rationale was economic,\(^{34}\) though political and security motives cannot be discounted given how regularly the fact that Viber was originally developed by an Israeli company was mentioned in the press. The committee never issued a recommendation on the subject. On November 3, 2013, responding to one newspaper’s allegations, the NTRA denied that it was considering imposing charges for Viber, WhatsApp, and BlackBerry Messenger use.\(^{35}\)

### Content Removal

Instances of direct government pressure on news sites to remove content are rare, but online journalists did report receiving a directive to refrain from reporting on an event in August 2014. A public prosecutor reportedly issued a gag order targeting news websites regarding the killing of four people by the police on the northern Alamein desert highway. This was the first instance of a media gag order that applied to online media alongside print.\(^{36}\)

---


\(^{33}\) “Egypt banks VoIP services from operators such as Skype,” BBC News, March 24, 2010, [http://bbc.in/1V0pZkD](http://bbc.in/1V0pZkD).


Media, Diversity, and Content Manipulation

Self-censorship is on the rise in the country. At a time when traditional media is suffering from what several independent newspaper editors have referred to as unseen level of homogeneity, online media is also struggling to maintain its independence.37 A survey by researchers at Northwestern University in Qatar found that only 25 percent of Egyptians agreed in 2015 that “The media can report the news independently without interference from officials,” down from 27 percent in 2013. Egypt ranked lower than Lebanon, Qatar, Saudi Arabia, Tunisia, and the UAE. Similarly, the amount of people who agreed “It is okay to express unpopular ideas on the internet” fell from 48 to 45 percent. 38 However, it did not appear that surveillance was having an effect on self-censorship, as the number of Egyptian individuals worried about government monitoring fell from 29 to 26 percent, the lowest figure of the six countries surveyed.

Online journalists have complained that while the state does not often exert pressure on news websites to censor, self-censorship is rife. Many are reluctant to cross redlines on sensitive topics, which include sectarian tensions, sexual liberty, the Muslim Brotherhood, detainees, and the military’s outsized role in the national economy. A provision in the August 2015 antiterrorism law criminalizes the publication of any information regarding militant attacks that contradicts official government statements, punishable by two years in prison.39 Those working for English-language outlets enjoy greater editorial freedom, while Arabic-language reporters fear that critical reports will affect their long-term professional prospects. Many experience online harassment from paid commentators. Those working for outlets affiliated with the Muslim Brotherhood face heavy prison sentences and can be accused of supporting a terrorist organization. 40

The Egyptian blogosphere has lost much of its vitality over the past few years. Attacks against bloggers have had a chilling effect; the increased popularity of Facebook and Twitter in the aftermath of the 2011 revolution has also led many key writers to focus their attention and content creation there. Registering a local .eg domain requires the submission of personal data and copies of a national ID, as well as a commercial registry for top level domains. Online websites are not recognized by the state as news outlets, unless connected to a print newspaper, making it tough to gain access to sources or fact-check information with officials. The Egyptian president has met occasionally with the editors-in-chief of the main news outlets, often admonishing them for not towing the line.

The economic viability of independent news websites is constantly under threat, as exemplified by the string of closures and financial difficulties experienced by most. The landscape is dominated by the online versions of state-owned newspapers or those benefiting from the backing of government-connected financiers.41 The most widely read news outlets, per the most recent Alexa ranking, are primarily tabloids and news portals aligned with the government.42

---

Egypt

Digital Activism

Digital activism and political organizing have been largely subdued over the past year due to fears of arrest, harsh jail sentences, and even murder by police forces while attending protests. A November 2013 law has effectively banned protest and given free rein to police in cracking down on demonstrations.43 Given the strong overlap of online and offline activism, especially for political activists, the chilling effect and the overall political disappointments that many have endured since 2011 have led to a decrease in political engagement, both on the streets and in writing. For instance, the website WikiThawra, the most reliable resource tracking numbers of imprisoned protesters, stopped operating in mid-2014, largely due its organizers’ disappointment in the current political situation.44

Violations of User Rights

While the Constitution formally guarantees freedom of speech, several new laws are threatening the expression of free ideas, both in the personal and the professional realm, with severe sentences. New cybercrime and antiterrorism laws were considered over the coverage period, with the latter passed in August 2015. Both laws include harsh penalties for online activities, which activists and observers warn could be used to prosecute dissidents and opposition political parties. Several users have been prosecuted over the coverage period for laws related to spreading chaos, insulting religion, or inciting debauchery. The monitoring of cyberspace by the authorities remains a high concern, and many worry that the establishment of a new High Council for Cybersecurity may lead to an increase in state surveillance against political opponents.

Legal Environment

The constitution, in effect since January 18, 2014,45 contains articles that address and nominally guarantee freedom of the press, stating that Egyptians “have the right to own and issue newspapers and establish visual, audio and digital media outlets.” According to Article 70, “the law shall regulate ownership and establishment procedures for visual and radio broadcast stations in addition to online newspapers.” This wording implies that even online sources of information could be regulated and their owners may be required to seek government approval in order to operate, as is currently the case with newspapers. Article 71 states that censorship is forbidden “in any way” and no individuals should be punished for publications. However, exceptions are made for “times of war or general mobilization,” with crimes delineated for “incitement to violence,” “discrimination amongst citizens, or impugning the honor of individuals.”46

Article 211 outlines the establishment of a “National Media Council” tasked with regulating “the af-
fairs of radio, television, and printed and digital press, among others” (Article 211) and ensuring that
the press maintains a commitment to “professional and ethical standards, as well as national security
needs.” Furthermore, Article 57 states that private communications “may only be confiscated, exam-
ined or monitored by causal judicial order, for a limited period of time, and in cases specified by the
law.” Judicial warrants are needed in order to enter, search, monitor, private property such as homes
as specified in Article 58. However the constitution continues to permit the trial of civilians under
military courts, to the anger of political activists. 47 Most of those trials occur outside of the capital
and away from the public eye.

During the coverage period, two legislative proposals posed a grave threat to internet freedom in
the country: the antiterrorism bill, first proposed in late 2013, 48 and the cybercrime law. The anti-
terrorism legislation classifies a larger number of crimes as terrorism and provides for the establish-
ment of a “Terrorism Prosecutor’s Office,” which would likely be subject to fewer checks and appeal
provisions than normal courts. One provision would allow the police to monitor internet traffic and
social media activity to “prevent their use for terrorist purposes.” 49 Furthermore, Article 27 calls for
a minimum sentence of five years in prison for “setting up a website with the goal of promoting
ideas or beliefs inciting to the use of violence, broadcasting information to mislead the police or
judicial authorities on terrorism cases, or exchanging messages and issuing orders between terrorist
groups or organizations.” 50 Setting up a group with the intention of “advocating by any means the
obstruction of provisions of the constitution or laws” is punishable by life imprisonment or the death
penalty, a charge that, activists pointed out, could apply to any peaceful political party or advocacy
group. 51 Finally, journalists face heavy fines for disputing official accounts of attacks by militants.

The antiterrorism bill was initially tabled for changes after coming under heavy criticism from the
international community; 52 however, the assassination of Prosecutor General Hisham Barakat on June
29, 2015 resulted in the draft being approved by the cabinet in one week 53 and ratified by the pres-
ident in August 2015. 54 Previously, President el-Sisi issued a separate law in February 2015 broaden-
ing the definition of “terrorist entities” to include anyone who threatens public order “by any means,”
and allowing the state to draw up lists of alleged terrorists or terrorist organizations. 55 The law was
met with wide skepticism from legal and rights activists, who criticized that the loose wording of the
law could allow the state to consider political parties, student unions, political movements, and hu-
man rights organizations as terrorist organizations. 56

A new cybercrime law was approved by the Council of Ministers in April 2015 and awaits ratification
by the president. The harbinger of this law was the 2014 constitution itself, which stated in article 34

48 “Draft Terrorism Law (full text);” [in Arabic], Al Masry Al Youm.
49 Al Hussaini,”Egypt’s Anti-Terrorism Law to Target Internet.”
50 Ibid.
51 Cairo Institute for Human Rights Studies, “Egypt’s draft anti-terrorism laws constitute greatest threat to civil liberties in 37
52 José Gonzalez, “Egyptian draft anti-terror laws pose a threat to freedom of expression,” Canadian Journalists for Free
Cunningham, “Egyptian draft laws to widen ‘terror’ definition drawing fierce criticism,” The Washington Post, April 22, 2014,
http://wapo.st/1QAuyBA.
east-33955894.
that “The security of cyberspace is an integral part of the economic system and national security. The State shall take the necessary measures to preserve it, as regulated by Law,” which led free speech activists at the time to warn of a potential crackdown on online freedom of expression. The draft law criminalizes insulting citizens or the state on the internet or on social media, as well as falsely attributing a website or email to someone else. It will also be used to combat incitement, terrorism, religious intimidation, and the use of personal photos and videos for blackmail. It allows law enforcement agencies to submit requests to block websites they deem to be a threat to “national security,” which has traditionally been used as an excuse to enforce censorship on political opponents, journalists, and activists. Article 98f of the law could also be used to prosecute dissenting political voices and human rights defenders on vague charges such as publishing news, information, or false rumors, if found to disturb public security, insult the president, mock monotheistic religions, or harm national unity or social peace. Penalties included in the draft law go up to life imprisonment without parole.57

Prosecutions and Detentions for Online Activities

Egyptians continue to face stark penalties for their online activities. The most concerning development over the past year was the sentencing of two online journalists to life imprisonment. At least two other users were given prison sentences for Facebook comments deemed to insult religion. Egypt’s LGBT community is also increasingly harassed by the police, including through the use of fake online dating profiles to entrap and arrest individuals for the crime of “debauchery.” Finally, well-known activist and blogger, Alaa Abdel Fattah, was sentenced to five years in prison for allegedly organizing a protest and assaulting a police officer in 2013 in a trial that many believe is politically motivated.

On April 11, 2015, a court in Cairo sentenced Abdullah al-Fakharany and Samhi Mustafa, respectively the executive director and cofounder of the news website Rassd, to life imprisonment. Mohamed al-Adly of the television station Ambad TV received the same sentence. The three had been held since August 25, 2013, when they were arrested after the dispersal of the pro-Mohamed Morsi sit-in at Rabaa Al-Adaweya square in Cairo. They were originally charged with “disturbing the peace,” but in February 2014 the General Prosecutor increased the charges to “spreading chaos” and “spreading false information” in the coverage of the dispersal.58 They were also charged with “forming an operations room to direct the Muslim Brotherhood to defy the government,” linking the news outlet to the Brotherhood, which has been banned as a terrorist organization.59 The trial took place before one of nine circuits allocated by the court of appeals to hear cases related to terrorism cases and those affecting “national unity and peace.”60

Numerous users were prosecuted for religious statements made online. On January 10, 2015, Karim Al-Banna was handed a three-year sentence on charges of “contempt of Islam and insulting the divine.” Al-Banna had declared his atheism on his Facebook page and was publicly harassed. He had

58 Committee to Protect Journalists, “Egypt sentences three journalists to life in prison,” April 11, 2015, http://cpj.org/x/5ff0.
been arrested in November 2014 while filing a police report related to the harassment he faced. After being released on bail pending appeal, he did not attend his retrial and is reportedly in hiding.

On February 16, 2015, Suez Canal University student Sherif Gaber was given a one-year sentence for contempt of religion on campus and atheist statements online. Following an argument with a professor in class, the professor printed and distributed posts from Gaber’s Facebook page where he discussed religion. He was reported by staff and students to the president of the university, who filed a legal complaint against him. Later, he was arrested from his home and reported having been subjected to torture while in custody.

The coverage period has also witnessed a renewed attack on the Egyptian LGBT community, both online and offline. In March 2015, it was reported that the police had arrested seven individuals believed to be transgender for the crime of debauchery, after using fake online dating profiles to organize a meetup. In September 2014, gay dating app Grindr disabled a geolocation feature in Egypt and displayed pop-up messages warning its Egypt-based users that the police was using the app to organize sting operations against LGBT users, urging them to be careful when sharing personal data and location.

Adlouah was not the only one arrested for a YouTube video. On May 25, 2015, belly dancer Reda El-Fouly was arrested and referred to a misdemeanor court on charges of ‘inciting debauchery and immorality’ after appearing in a racy low-budget video clip uploaded to the internet. Her boyfriend Wael El-Sedeky, who appears in the clip and directed it, was also charged but remains out of the country.

Finally, the legal harassment of Alaa Abdel Fattah, a prominent blogger and leading figure in the 2011 revolution, continues. On February 23, 2015, Abdel Fattah was sentenced, along with 24 other defendants, to prison for five years for a brief protest on November 26, 2013 against newly passed legislation that criminalized assembly and protests without government permission. Two days after the protest was dispersed with teargas and water cannons, police raided Abdel Fattah’s house, assaulted him and his wife, and arrested him. Abdel Fattah was accused of organizing the protest on Twitter. The trial was highly politicized. After his original arrest and subsequent release for retrial, he and another defendant were barred entry to the court proceedings during which they were sen-
Alaa is currently in a high-security prison.

**Surveillance, Privacy, and Anonymity**

Surveillance and monitoring are a wide concern in the country, given the tense environment in which numerous users have been arrested for their online activities. On June 1, 2014, *al-Watan* published a leaked document that revealed the Egyptian Ministry of Interior was looking to purchase technology to conduct real-time monitoring of social media and communication apps such as Facebook, Twitter, Viber, and WhatsApp. In a “call for tenders” document, the government requested a Social Networks Security Hazard Monitoring System to penetrate public and private communications in order to monitor for a long list of ‘hazards’ and ‘destructive ideas’ online. The list was broad and included things such as “calling for normalizing relations with enemies,” “spreading myths and claims of miracles,” “spreading rumors and intention misrepresentation of facts,” and “pornography, looseness, and immorality.” A coalition of human rights organizations filed a lawsuit in June 2014 to call for a halt to the tender. It was later reported that “SEE Egypt,” a reseller of Blue Coat technology in Egypt, had been contracted to provide the monitoring tools. The company reportedly listed the ministries of interior and defense as its clients, which it subsequently denied, though news articles reported quotes from an official press release posted to its homepage. The company removed its website altogether for several days.

Egypt is known to already possess sophisticated surveillance tools. In February 2014, researchers from the University of Toronto’s Citizen Lab identified the Egyptian government as a user of “Remote Control System” (RCS), a spyware technology. Produced by the Milan-based company “Hacking Team,” RCS is marketed as “the hacking suite for governmental interception” and can capture data on the target’s computer; monitor encrypted internet communications; record Skype calls, emails, messages, and passwords typed into a browser; and remotely turn on a device’s webcam and microphone. RCS operates by infecting a target’s device, most likely through phishing; data stolen is transferred through multiple ‘hops’ to anonymize the packets and distance the spying government. Researchers identified Egypt-based endpoints for the reception of data channeled by RCS, indicating it was operational under the current military-led regime. In July 2015, a leak of Hacking Team documents confirmed this, with invoices showing that the Egyptian Ministry of Defense, and possibly

71 According to an unofficial English translation, the list also includes “blasphemy and skepticism in religions; regional, religious, racial, and class divisions; throwing accusations; libel; insulting sarcasm; calls for the disregard of societal pillars; encouraging extremism, violence and dissent; mobilizing for demonstrations, sit-ins and illegal strikes; educating about making explosives as well assault, chaos and riot tactics; fishing for honest mistakes; stalking intimacies; and taking statements out of context”. For the full text of the tender, see [http://www.elwatannews.com/news/details/495659](http://www.elwatannews.com/news/details/495659) [in Arabic]; Ministry of Interior, *Social Networks Security Hazard Monitoring Project Booklet*, [http://bit.ly/1NzlJt7](http://bit.ly/1NzlJt7).
other institutions, paid EUR 737,500 ($845,000) to the company through a third-party intermediary.\(^7\) Previously, protestors who broke into one of Egypt’s intelligence agencies found documents showing that the government had received surveillance and hacking products from Gamma and Narus, a subsidiary of Boeing.\(^7\) There is no independent oversight authority to monitor the use of internet surveillance by the police.

Several regulations on SIM card registration or the use of anonymizers restrict the ability of Egyptians to use the internet anonymously. Mobile phone customers must provide their National ID numbers to their providers. On July 20, 2014, the NTRA issued additional guidelines compelling mobile companies to ensure their customers register, promising stricter oversight and a review of mobile operators’ databases to ensure compliance. Consequently, during the course of 2014, operators directed to present themselves in person to a company outlet to review their data. The Cairo Chamber of Commerce has suggested that a main cause for the laxity in registration has been due to actions of resellers, whom mobile operators provide with unregistered lines and subsequently fail to oversee. This had led vendors to complete paperwork with fake names and ID numbers, or with the data of previous clients. The issue took an additional sense of urgency with the growing use of mobile-detonated explosives in Egypt over the past year.\(^8\) On January 27, 2015, the Cairo Court for Urgent Matters ruled that unregistered lines should be suspended.\(^9\) The Court of Appeals confirmed this ruling on April 27.\(^10\)

Encryption is also restricted within the country. According to the Egyptian Telecommunications Law, “telecommunication services operators, providers, their employees and Users of such services shall not use any Telecommunication Services encryption equipment except after obtaining a written consent from each of the NTRA, the Armed Forces and National Security Entities, and this shall not apply to encryption equipment of radio and television broadcasting.”\(^11\)

Cooperation between private companies and the government in handing over user data is thought to be extensive. ISPs and mobile operators are obliged to maintain a database of their customers and allow government access to their databases. In the past, details emerged that mobile operators Vodafone, Mobinil, and Etisalat had to sign terms of agreement that bound them to cooperate with government officials when requested to tap any conversation or monitor any discussion. In an interview, Mobinil founder Naguib Sawiris stated that under the company’s terms of agreement, the government had the right to cancel any or all mobile services in the absence of cooperation.\(^12\)

---

83 Telecommunication Regulation Law No. 10.
**Intimidation and Violence**

In a continuing trend, this year saw several sectarian attacks in retribution for Facebook posts deemed to insult religion. The perpetrators of this type of violence are rarely held accountable, with the police or judiciary turning a blind eye and sometimes targeting victims rather than aggressors. In late May 2015, 18 members of 5 Christian families from a village in Upper Egypt were expelled from their homes after one man allegedly published a Facebook post insulting the prophet Mohamed. Groups of villagers gathered outside their houses and demanded they leave the village, all under the approval of security forces. According to the TV presenter who broke the story nationally, the man accused of writing the post is in fact illiterate.85

**Technical Attacks**

Technical violence is not widespread, with only a few instance of hacking and defacement reported during the past year. In April 2015, hacker forums reported that some minor Egyptian government websites had been defaced, with the photo of former president Morsi posted on the homepage.86 In March 2015, it was uncovered that an Egyptian intermediate certificate authority had issued unauthorized digital certificates for several Google domains, allowing it to potentially act as a “man-in-the-middle.”87 The company, MCS Holdings, had issued the certificates from CNNIC (the Chinese Internet Network Information Center), under the pretense—according to the latter—that they would only be issued for domains held by MCS.88 Upon discovery, Google blocked the certificates with a CRLSet push, an emergency failsafe measure designed to revoke unauthorized certificates. MCS, which defines itself as “one of the major security products distributers in Egypt and the Middle East” issued a statement saying it was a “human mistake.”89 Google noted that there was “no indication of abuse” and that it was “considering what further actions are appropriate.”

In December 2014, Egypt established the High Council for Cybersecurity (HCC) to protect vital national infrastructure from cyberattacks. The HCC is mainly composed of representatives from various ministries, the central bank, and the intelligence service, and is headed by the minister of communications and information technology. Reports of hacking were very prominent in 2013, with the websites of Rassd and the April 6th Youth Movement attacked. Some activists have expressed concerns that the HCC could be used to monitor the political activities of government critics, particularly since its by-laws have yet to be established.90

Key Developments: June 2014 – May 2015

- Estonia continues to be one of the most wired countries in the world, with increasing internet access and online participation among citizens (see Availability and Ease of Access).

- In June 2015, the European Court of Human Rights upheld an Estonian Supreme Court decision from 2009 stating that content hosts may be held legally liable for third-party comments made on their website (see Content Removal).

- Estonia continues to improve protections for the right to privacy, with the Ombudsman playing an increasingly active role in supporting privacy rights related to digital data and communications (see Surveillance, Privacy, and Anonymity).
FREEDOM
ON THE NET
2015

Estonia

Introduction
Estonia in one of the most wired and technologically advanced countries in the world. With a high
internet penetration rate, widespread e-commerce, and e-government services embedded into the
daily lives of individuals and organizations, Estonia has become a model for free and open internet
access as a development engine for society. When the country regained independence in 1991 after
nearly 50 years of Soviet rule, its infrastructure was in a disastrous condition. The country’s new leadership, however, perceived the expansion of information and communication technologies (ICTs) as a
key to sustained economic growth and invested heavily in their development.
After the first internet connections in the country were introduced in 1992 at academic facilities in
Tallinn and Tartu, the government further worked with private and academic entities to initiate a program in 1996 called Tiger Leap, which aimed to establish computers and internet connections in all
Estonian schools by 2000. This program helped to build a general level of technological competence
and awareness of ICTs among Estonians. Today, with a high level of computer literacy and connectivity already established, the program’s focus has shifted from basic concerns such as access, quality,
and cost of internet services to discussions about security, anonymity, the protection of private information, and citizens’ rights on the internet. In addition, the majority of users conduct business and
e-government transactions over the internet: in 2013, nearly 97 percent of banking transactions were
done with e-banking services, and 95 percent of people declared their income electronically.1
With regard to ensuring freedom of expression, recent court rulings on intermediary liability in Estonia have posed some concerns. On June 16, 2015, the Grand Chamber of the European Court of
Human Rights issued a ruling that reaffirmed an earlier Estonian Supreme Court decision regarding
the legal liability of content hosts for third-party comments. The Grand Chamber of the ECtHR found
that a company’s legal liability for comments posted by its users did not sufficiently interfere with
the freedom of expression guarantees enshrined in the European Convention on Human Rights;
therefore, intermediaries could be held responsible for third-party content published on their website or forum, even if they delete the content upon notification.2
Additionally, over the past year, the issue of privacy for individual users on the internet became
a widely debated topic in Estonia, with a particular focus on the privacy policies of global service
providers. The Digital Agenda 2020 for Estonia, established by the Ministry of Economic Affairs and
Communications, outlines how both technological and organizational conditions will be developed
to ensure that people will always know and be able to decide when, by whom, and for what purpose
their personal data is being used in the public sector.3 The same agenda also launched an “e-residency” program to offer its secure and convenient online services to the citizens of other countries.
Services include digital authentication, digital signage of documents, encryption and transmission
of the documents and other electronic communication, and access to all Estonian public and private
sector online services.4


1

id”:[“001-155105”]}

2

3


4


283

www.freedomhouse.org


Estonia

Obstacles to Access

Estonia continues to be one of the most connected countries in the world with regard to internet access, and Estonian internet users face very few obstacles when it comes to accessing the internet.

Availability and Ease of Access

The number of internet and mobile telephone users in Estonia has grown rapidly in the past 20 years. According to statistics from the International Telecommunication Union (ITU), internet penetration in Estonia reached 84 percent in 2014, compared to 79 percent in 2013 and 73 percent in 2008.\(^5\) There were also over 2 million mobile phone subscriptions, translating to a mobile phone penetration rate of 160 percent.\(^6\) This figure is commonly attributed to the widespread use of mobile internet access devices, the growing popularity of machine-to-machine (M2M) services, and the use of more than one mobile phone by individual Estonians.

The first public Wi-Fi area was launched in 2001, and since then the country has developed a system of mobile data networks that enable widespread wireless broadband access. In 2011, the country had over 2,440 free, certified Wi-Fi areas meant for public use, including at cafes, hotels, hospitals, schools, and gas stations, and the government has continued to invest in public Wi-Fi.\(^7\) In addition, a countrywide wireless internet service based on CDMA technology has been deployed and is priced to compete with fixed broadband access. Three mobile operators cover the country with mobile 3G and 3.5G services, and as of May 2015, 4G services covered over 97 percent of Estonian territory. Municipalities in rural areas have been subsidizing local wireless internet deployment efforts, and the country's regulatory framework presents low barriers to market entry, enabling local startups to proliferate.

Estonians use a large variety of internet applications, including search engines (85 percent of users), email (83 percent of users), local online media, news portals, social-networking sites, instant messaging, and Voice over Internet Protocol (VoIP) services.\(^8\) Estonian Public Broadcasting delivers all radio channels and its own TV production services, including news in real time over the internet; it also offers archives of its radio and television programs at no charge to users.

Restrictions on Connectivity

There were no government-imposed restrictions or disruptions to internet access during the past year.

---

\(^5\) International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2015, accessed June 1, 2015, [http://www.itu.int/net4/itu-d/icteye/](http://www.itu.int/net4/itu-d/icteye/).


Estonia

ICT Market

The Estonian Electronic Communications Act was passed in late 2004, and a number of amendments have been added to help develop and promote a free market and fair competition in electronic communications services.\(^9\) Today, there are over 200 operators offering such services, including six mobile operators and numerous internet service providers (ISPs). ISPs and other communications companies are required to register with the Estonian Technical Surveillance Authority (ETSA), a branch of the Ministry of Economic Affairs and Communications, though there is no registration fee.\(^10\)

Regulatory Bodies

In 2009, the Estonian Internet Foundation was established to manage Estonia’s top level domain, “.ee.”\(^11\) With its multi-stakeholder foundation, the organization represents the Estonian internet community internationally and has succeeded in overseeing various internet governance issues such as the domain name registration process. After initial concerns over the foundation’s domain registration pricing policy\(^12\) and management capabilities,\(^13\) the foundation’s substantive work was stabilized in 2012-2013. In February 2012, the Estonian Internet Foundation was admitted to the Council of European National Top Level Domain Registries (CENTR). During last three years the domain registration and annual fees have dropped from a €20 annual fee to a €9 annual fee, together with a 40 percent decrease in the registrar’s deposit, a decrease in the registrar’s service fees, and an unlimited number of domains for each user.\(^14\)

Limits on Content

Estonians have access to a wide range of content online, and very few resources are blocked or filtered by the government. However, a 2009 court ruling on intermediary liability for third-party comments, which has subsequently been upheld by several European Court of Human Rights decisions, has the potential to increase instances of censorship or removal of content, particularly on forums or other websites with public comment sections.

Blocking and Filtering

There are very few restrictions on internet content and communications in Estonia. YouTube, Facebook, Twitter, LinkedIn and many other international video-sharing and social-networking sites are widely available and popular. Estonians use the internet for uploading and sharing original content

---

12 The activities of the Estonian Internet Foundation are not subsidized from the state budget; the registration fee covers infrastructure investments, operating costs, and reserve funds.
such as photographs, music, and text—a higher percentage of people in Estonia (32 percent) use the internet to publically share self-created content than do people in any other country in Europe.\textsuperscript{15}

In January 2010, a new law on online gambling came into force, requiring all domestic and foreign gambling sites to obtain a special license or face access restrictions. As of February 2014, the Estonian Tax and Customs Board had over 1,000 websites on its list of illegal online gambling sites that Estonian ISPs are required to block.\textsuperscript{16} The list of blocked sites is transparent and available to the public.

\section*{Content Removal}

Due in part to Estonia’s strong privacy laws, there have been some instances of content removal related to online communications. Most of these cases involve civil court orders to remove inappropriate or off-topic reader comments from online news sites. Comments are also sometimes removed from online discussion forums and other sites. Generally, users are informed about a given website’s privacy policy and rules for commenting, which they are expected to follow. Most of the popular online services have established policies that outline a code of conduct for the responsible and ethical use of their services and have enforcement policies in place.

In 2008, a debate over pre-publication censorship took center stage when the victim of unflattering and largely anonymous comments on a news story filed suit against the popular Estonian news site Delfi, claiming that the web portal must be held responsible for defamatory reader comments and screen them before they become public.\textsuperscript{17} In 2009, the Estonian Supreme Court upheld the rulings of the lower courts, stating that Delfi is not a passive intermediary since the site already exerts control over the comments section by removing those that violate their own rules; therefore, it can be held liable for defamatory or otherwise illegal content prior to publication. Website owners argued that they did not have the capacity to monitor and edit all comments made on their sites.

In October 2013, the European Court of Human Rights upheld the Estonian Supreme Court ruling by stating that the company’s liability for defamatory comments was not a “disproportionate interference” with Article 10 of the European Convention on Human Rights, which guarantees freedom of expression.\textsuperscript{18} The case was then referred to the Grand Chamber of the European Court of Human Rights, which also upheld the decision, stating in June 2015 that content hosts may be held legally liable for third-party comments made on their website.\textsuperscript{19}

\begin{flushright}
\begin{itemize}
\item \textsuperscript{15} “Individuals Using the Internet for Uploading Self-Created Content to Any Website to Be Shared,” Eurostat, accessed June 11, 2013, http://appsso.eurostat.ec.europa.eu.
\item \textsuperscript{17} Kaja Koovit, “Big Businessman Goes to War Against Web Portals,” Baltic Business News, March 18, 2008, http://www.balticbusinessnews.com/?PublicationId=48694078-50cc-4fe1-b3e4-6e10dcb6a5ec1.
\item \textsuperscript{19} “CASE OF DELFI AS v. ESTONIA,” Grand Chamber judgment, http://hudoc.echr.coe.int/eng?i=001-155105# (“item id”:”001-155105”), accessed June 18, 2015
\end{itemize}
\end{flushright}
Estonia

Media, Diversity, and Content Manipulation

Estonians have access to a wide array of content online, and there are few economic or political barriers to posting diverse types of content, including different types of news and opinions.

Additionally, Estonia has the largest functioning public-key infrastructure\(^{20}\) in Europe, based on the use of electronic certificates maintained on the national identification (ID) card.\(^{21}\) More than 1.2 million active ID cards are in use, which enable both electronic authentication and digital signing, and over 40 percent of active ID cards have been used for these purposes.\(^{22}\) The Digital Signature Act, adopted in 2000,\(^{23}\) gives an individual’s digital signature the same weight as a handwritten one and requires public authorities to accept digitally-signed documents. Estonian ID cards were used to facilitate electronic voting during the parliamentary elections in 2007 and were used again in the 2009 municipal and European Parliament elections. During the 2014 European Parliament elections, 103,151 votes were cast over the internet, representing over 31 percent of all votes from Estonia.\(^{24}\) In 2013, 95 percent of citizens filed their taxes online, making the web services offered by the tax department the most popular public e-service. Over 63 percent of internet users regularly use e-government services, and 77 percent of these users have indicated their satisfaction with such services.\(^{25}\)

Digital Activism

Social media use in Estonia is fairly widespread, and Estonians often make use of such sites to share news and information, and to generate public discussion about current political debates. One of the more well-known examples of digital activism came in early 2012, when Estonian daily newspapers and TV raised public awareness on the progress of the Anti-Counterfeiting Trade Agreement (ACTA) and its developments in the European Union. As in many other countries, the Estonian government's initial position on ACTA's possible negative implications on user privacy was formal, stating that nothing would change if ACTA were ratified.\(^{26}\) From February 8-20, 2012, the discussion on ACTA escalated in public media and political debates, which were crucially influenced by the internet user community and experts. On February 11\(^{27}\), demonstrations against ACTA in Tallinn and Tartu gathered more than 2,000 participants. As a result, open debates in the Estonian Parliament rephrased the government’s initial support with a more careful approach to be informed by further consultations and analysis. Overall, the ACTA controversy in Estonia demonstrated the increasing influence of civic participation on internet freedom issues and intellectual property regulation.

\(^{20}\) A public-key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates, which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates that map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed.

\(^{21}\) See the web portal for the ID-card system, [http://id.ee/?lang=en](http://id.ee/?lang=en).

\(^{22}\) See the web portal for the ID-card system, [http://id.ee/?lang=en](http://id.ee/?lang=en).


Violations of User Rights

Freedom of speech and freedom of expression are protected by Estonia’s constitution and by the country’s obligations as a member state of the European Union. Anonymity is unrestricted, and there have been extensive public discussions on anonymity and the respectful use of the internet. Internet access at public access points can be obtained without prior registration. Over the past few years, the government has succeeded in reducing the number and severity of cyberattacks against its infrastructure.

Legal Environment

According to the constitution of Estonia, everyone has the right to freely obtain information and to freely disseminate ideas, opinions, beliefs, and other information. In addition, everyone has the right to the confidentiality of messages sent or received. In general, these rights are well protected. Any restrictions on these rights must be necessary in a democratic society and shall not distort the nature of the rights and freedoms restricted.28

The incitement of national, racial, religious or political hatred, violence, or discrimination is also prohibited and punishable by law. Estonia is currently in the process of amending the penal code to establish a framework on hate speech criminalization in the country and thereby comply with the European Council Framework Decision 2008/913/JHA,29 issued November 28, 2008, on “combating certain forms and expressions of racism and xenophobia by means of criminal law.” In July 2012, the Ministry of Justice initiated proceedings to amend sections 151 and 152 of the penal code, which would lead to a new legal norm regarding hate speech-related legislation in Estonia.30 This process is still ongoing and has become the topic of significant public debate within the country.

Prosecutions and Detentions for Online Activities

There were no cases of prosecutions or detentions for online activities during the coverage period.

Surveillance, Privacy, and Anonymity

The Personal Data Protection Act (PDPA), first passed in 1996, restricts the collection and public dissemination of an individual’s personal data. No personal information that is considered sensitive—such as political opinions, religious or philosophical beliefs, ethnic or racial origin, sexual behavior, health, or criminal convictions—can be processed without the consent of the individual. The Data Protection Inspectorate (DPI) is the supervisory authority for the PDPA, tasked with ‘state supervi-

---

In 2015, the Chancellor of Justice (Ombudsman) processed several cases related to online privacy and data protection. The Ombudsman is an independent official whose duties are to ensure that legislation in Estonia complies with the constitution, and that the fundamental rights and freedoms of the Estonian people are protected. In three cases during the spring of 2015, the Chancellor strongly and clearly argued for the users’ right to privacy with regard to the protection of private data in public databases. The Chancellor of Justice’s office has taken a leading role in interpreting the constitution in cases related to privacy and private information on the internet in Estonia, establishing new standards for the protection of user rights online.

Estonia launched the Electronic Communications Act on January 1, 2005, aligning itself with EU legislation and replacing the Telecommunications Act. Since January 2008, electronic communications companies have been required to preserve traffic and location data for one year, as defined by the EU Data Retention Directive (2006/24/EC). Companies have been required to retain data on internet access, telephony, and email since March 2009, and must only retain the data that becomes known to them in the course of providing communications services. They must also provide the surveillance agency or security authority with the information at their disposal only when presented with a court order.

However, data retention practices in Estonia and other European Union member states were recently thrown into doubt by the European Court of Justice (ECJ). On April 8, 2014, the court found the European Data Retention Directive (2006/24/EC) to be invalid and in contravention of articles 7, 8, and 52(1) of the European Convention on Human Rights. The ruling was lauded among privacy proponents who had long argued that requirements for the blanket retention of data constituted mass surveillance and far exceeded what was necessary for law enforcement purposes. However, the decision has also prompted debate among legal experts and different reactions by governments, with some member states now suspending their national implementations of the European directive, while others are drafting new data retention laws in order to compel internet service providers to continue to store user data.

According to a report by the Estonian Parliament Security Authorities Surveillance Select Committee, which oversees the practices of surveillance agencies and security agencies, there were over 7,400 cases of information requests based on court orders in 2012, an increase of 9 percent from the previous year. The select committee was established to exercise supervision over the legality of surveil-

35. The ECJ court ruling pertained to the cases Digital Rights Ireland Ltd (C-293/12) and Kärntner Landesregierung (C-594/12) and is available at http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.
Estonia

lance and the activities of the Security Police. The committee monitors the activities of the Security Police Board to ensure conformity with the constitution, the Surveillance Act, and other regulations on security agencies.

Intimidation and Violence

There have been no physical attacks against bloggers or online journalists in Estonia, though online discussions are sometimes inflammatory. Following instances of online bullying, sexual harassment, and the misuse of social media in 2009-2010, discussions and public awareness campaigns were launched to involve parents in increasing the protection of children on the internet.

Technical Attacks

Awareness of the importance of ICT security in both private and business use has increased significantly since a series of cyberattacks against Estonian websites and government organizations in the spring of 2007. To protect the country from future attacks, the government adopted a five-year Cyber Security Strategy in 2008 that focused on the development and implementation of new security measures that would increase competence in cyber security, improve the legal framework, bolster international cooperation, and raise public awareness. Estonia’s cybersecurity strategy is built on strong private-public collaboration and a unique voluntary structure through the National Cyber Defense League. With more than 150 experts participating, the league has simulated different security threat scenarios as defense exercises that have served to improve the technical resilience of Estonia’s telecommunication networks and other critical infrastructure over the past few years.

Also in 2008, the North Atlantic Treaty Organization (NATO) established a joint cyberdefense center in Estonia to improve cyberdefense interoperability and provide security support for all NATO members. Since its founding, the center has supported awareness campaigns and academic research on the topic and hosted several high-profile conferences, among other activities. From 2009, the NATO Cooperative Cyber Defense Centre of Excellence has organized an annual International Conference on Cyber Conflict, or CyCon, bringing together international experts from governments, the private sector, and academia. CyCon has focused on international cooperation and the legal, regulatory, military, and paramilitary aspects of cybersecurity, with the goal of ensuring the development of a free and secure internet.

Key Developments: June 2014 – May 2015

- A significant number of service interruptions in the name of routine maintenance and system updates resulted in worsening service across the country. Internet services on 3G mobile internet networks were reportedly unavailable for more than a month in July and August 2014 (see Restrictions on Connectivity).

- A growing number of critical news and opposition websites were blocked in the lead up to the May 2015 elections (see Blocking and Filtering).

- Six bloggers of the prominent Zone 9 blogging collective arrested in April 2014 were officially charged with terrorism in July 2014; two of the bloggers were unexpectedly released and acquitted in July 2015, joined by the four others in October (see Prosecutions and Detentions for Online Activities).

- A university political science teacher known for his Facebook activism and another blogger were arrested and charged with terrorism in July 2014, among three others (see Prosecutions and Detentions for Online Activities).

- Online journalists in the Ethiopian diaspora were attacked with Hacking Team’s sophisticated surveillance malware (see Technical Attacks).
Introduction

Ethiopia, the second most populated country in sub-Saharan Africa, has one of the lowest rates of internet and mobile phone connectivity in the world. Telecommunication services, in general, and the internet, in particular, are among the most unaffordable commodities for the majority of Ethiopians, as poor telecom infrastructure, the government’s monopoly over the information and communication technologies (ICTs) sector, and obstructive telecom policies have significantly hindered the growth of ICTs in the country, making the cost of access prohibitively expensive.

Despite the country’s extremely poor telecommunications services and a largely disconnected population, Ethiopia is also known as one of the first African countries to censor the internet, beginning in 2006 with opposition blogs.\(^1\) Since then, internet censorship has become pervasive and systematic through the use of highly sophisticated tools that block and filter internet content and monitor user activity. The majority of blocked websites feature critical news and opposition viewpoints run by individuals and organizations based in the diaspora. In the lead up to the May 2015 general elections, a growing number of critical news and opposition websites were blocked, while select tools, such as Storify and a popular URL shortening tool Bitly, remained blocked throughout the year. The government also employs commentators and trolls to proactively manipulate the online news and information landscape, and surveillance of mobile phone and internet networks is systematic and widespread.

In 2014–15, the Ethiopian authorities increased their crackdown on bloggers and online journalists, using the country’s harsh laws to prosecute individuals for their online activities and quash critical voices. The Zone 9 bloggers arrested in April 2014 were charged with terrorism in July 2014 and subsequently subjected to a series of sham trials through mid-2015. In July 2015, two of the imprisoned Zone 9 bloggers were unexpectedly released and acquitted of all charges, which observers attributed to U.S. President Barack Obama’s official visit to the country later that month. The four remaining Zone 9 bloggers were acquitted in October. Nevertheless, five other critical voices and bloggers who were arrested in July 2014 and charged with terrorism remain in prison. During the numerous Zone 9 trials throughout 2014–2015, several supporters were temporarily arrested for posting updates and pictures of their trials on social media via mobile devices.

Obstacles to Access

A significant number of service interruptions in the name of routine maintenance and system updates resulted in worsening service across the country. Internet services on 3G mobile internet networks were reportedly unavailable for more than a month in July and August 2014.

Availability and Ease of Access

In 2015, access to ICTs in Ethiopia remained extremely limited, hampered by slow speeds and the

---

Ethiopia

state’s tight grip on the telecom sector. According to the International Telecommunications Union (ITU), internet penetration stood at a mere 3 percent in 2014, up from just 2 percent in 2013. Only 0.5 percent of the population had access to fixed-broadband connections, increasing from 0.25 percent in 2013. Ethiopians had more access to mobile phone services, with mobile phone penetration rates increasing from 27 percent in 2013 to 32 percent in 2014, though such access rates still lag behind an estimated regional average of 74 percent and cell phone ownership is much more common in urban areas than rural areas. Meanwhile, less than 5 percent of the population has a mobile-broadband subscription as of the latest available data from 2013. In March 2015, Ethiopia’s single telecoms provider, the state-owned EthioTelecom, announced it had launched 4GLTE mobile technology in the capital Addis Ababa, but the service is reportedly only available to a mere 400,000 subscribers. Radio remains the principal mass medium through which most Ethiopians stay informed.

While access to the internet via mobile phones increased slightly in the past year, prohibitively expensive mobile data packages still posed a significant financial obstacle for the majority of the population in Ethiopia, where per capita income stood at US$470 as of the latest available data from 2013. Ethiopia’s telecom market is highly undeveloped due to monopolistic control, providing customers with few options at arbitrary prices, which are set by the state-controlled EthioTelecom and kept artificially high. As of mid-2015, monthly packages cost between ETB 200 and 3,000 (US$10 to $150) for 1 to 30 GB of 3G mobile services.

The combined cost of purchasing a computer, setting up an internet connection, and paying usage charges makes internet access beyond the reach of most Ethiopians. Consequently, only 2 percent of Ethiopian households have fixed-line internet access in their homes. While access via mobile internet is increasing, the majority of internet users still rely on cybercafes to log online. A typical internet user in Addis Ababa pays between ETB 5 and 7 (US$0.25 to $0.35) for an hour of access. Because of the scarcity of internet cafes outside urban areas, however, rates in rural cybercafes are more expensive.

For the few Ethiopians who can access the internet, connection speeds are known to be painstakingly slow and have not improved in years, despite rapid improvements everywhere else around the world. Logging into an email account and opening a single message can still take as long as six minutes at a standard cybercafe with broadband in the capital city—the same rate reported over the past few years—while attaching documents or images to an email can take as long as eight minutes.

12 International Telecommunication Union, “Ethiopia Profile (Latest data available: 2013),”
Ethiopia

or more.\(^{13}\) According to May 2015 data from Akamai’s “State of the Internet” report, Ethiopia has an average connection speed of 1.8 Mbps (compared to a global average of 3.9 Mbps).\(^{14}\)

Despite reports of massive investments from Chinese telecom companies in recent years,\(^{15}\) Ethiopia’s telecommunications infrastructure is among the least developed in Africa and is almost entirely absent from rural areas, where about 85 percent of the population resides. There are only a few signal stations across the country, resulting in frequent network congestions and disconnections, even on state controlled media.\(^{16}\) Consequently, many people often use their cell phones as music players or cameras. In a typical small town of Ethiopia, individuals often hike to the top of their nearest hills to access a signal for a mobile phone call. Frequent electricity outages also contribute to poor telecom services.

Restrictions on Connectivity

The Ethiopian government’s complete control over the country’s telecommunications infrastructure via EthioTelecom enables it to restrict access to the internet and mobile phone services. Ethiopia is connected to the international internet via satellite, a fiber-optic cable that passes through Sudan and connects to its international gateway, and the SEACOM cable that connects through Djibouti to an international undersea cable. All connections to the international internet are completely centralized via EthioTelecom, enabling the government to cut off the internet at will. As a result, the internet research company Renesys classified Ethiopia “as being at severe risk of Internet disconnection,” alongside Syria, Uzbekistan, and Yemen in a February 2014 assessment.\(^{17}\)

There were a significant number of service interruptions throughout the year in the name of routine maintenance of network infrastructure and system updates across the country, resulting in worsening service. Numerous users reported extremely slow internet and text messaging speeds during the coverage period, and internet services on EVDO and CDMA networks were reportedly unavailable for more than a month in July and August 2014.\(^{18}\)

In a sample test conducted in March 2015 to measure the frequency and pervasiveness of mobile network interruptions, 40 to 60 percent of phone calls dropped in the middle of conversation.\(^{19}\) Nearly 70 percent of the time, testers needed to make prolonged and repeated attempts for their calls to go through. Text messaging services were also found to be extremely poor and slow. The same sample test found that it took an average of six minutes to send a text message to ten individuals, while replies varied from one to six minutes. Approximately 30 percent of text messages were not delivered to the intended recipient at all. The test further found that 60 percent of mobile phone users frequently ran out of their prepaid mobile data allowances prematurely.

\(^{13}\) According to tests by Freedom House consultant in 2015.
\(^{15}\) Aaron Maasho, "Ethiopia signs $700 mln mobile network deal with China's Huawei," Reuters, July 25, 2013, [http://reuters.rs/1OpDgVj](http://reuters.rs/1OpDgVj).
\(^{18}\) Freedom House interviews.
\(^{19}\) Conducted by Freedom House consultant, March 2015.
Ethiopia

ICT Market

The space for independent initiatives in the ICT sector, entrepreneurial or otherwise, is extremely limited, with state-owned EthioTelecom holding a firm monopoly over internet and mobile phone services as the country's sole telecommunications service provider. Despite repeated international pressure to liberalize telecommunications in Ethiopia, the government refuses to ease its grip on the sector.

China is a key investor in Ethiopia's telecommunications industry, with Zhongxing Telecommunication Corporation (ZTE) and Huawei currently serving as contractors to upgrade broadband networks to 4G in Addis Ababa and to expand 3G across the country. The partnership has enabled Ethiopia's authoritarian leaders to maintain their hold over the telecom sector, though the networks built by the Chinese firms have been criticized for their high cost and poor service. Furthermore, the contracts have led to increasing fears that the Chinese may also be assisting the authorities in developing more robust ICT censorship and surveillance capacities. In December 2014, the Swedish telecom group Ericsson emerged as the latest partner to improve and repair the quality of Ethiopia's mobile network infrastructure, though China's ZTE still maintains the lion's share of the telecom infrastructure investment sector.

Meanwhile, onerous government regulations stymie other aspects of the Ethiopian ICT market. For one, imported ICT items are tariffed at the same heavy rate as luxury items, unlike other imported goods such as construction materials and heavy duty machinery, which are given duty-free import privileges to encourage investments in infrastructure. Ethiopians are required register their laptops and tablets at the airport with the Ethiopian customs authority before they travel out of the country, ostensibly to prevent individuals from illegally importing electronic devices, though observers believe the requirement is an effort to keep tabs on the ICT activities of Ethiopian citizens.

Local software companies in the country have also suffered from heavy-handed government regulations, which do not have fair, open, or transparent ways of evaluating and awarding bids for new software projects. Government companies are given priority for every kind of project, while smaller entrepreneurial software companies are completely overlooked, leaving few opportunities for local technology companies to thrive.

---

Meanwhile, cybercafes are subject to onerous operating requirements under the 2002 Telecommunications (Amendment) Proclamation, which requires cybercafe owners to obtain an operating license with EthioTelecom via a murky process that can take months. In the past few years, EthioTelecom began enforcing its licensing requirements more strictly in response to the increasing spread of cybercafes, reportedly penalizing Muslim cafe owners more harshly. Violations of the stringent requirements, such as a prohibition on providing Voice-over-IP (VoIP) services, entail criminal liability, though there have been no reported violations to date.

Regulatory Bodies

Since the emergence of the internet in Ethiopia, the Ethiopian Telecommunications Agency (ETA) has been the primary regulatory body overseeing the telecommunications sector. In practice, executives in the government have complete control over ICT policy and sector regulation. The Information Network Security Agency (INSA), a government agency established in 2011 and controlled by individuals with strong ties to the ruling regime, also has significant power in regulating the internet under the mandate of protecting the country's communications infrastructure and preventing cybercrimes in the country.

Limits on Content

Dozens of critical news and opposition websites and blogs were blocked as the country prepared for the general elections in May 2015. Over 100 websites remained blocked overall. The activities of pro-government commentators noticeably increased during the coverage period.

Blocking and Filtering

The Ethiopian government imposes nationwide, politically motivated internet blocking and filtering that tends to tighten ahead of sensitive political events. The majority of blocked websites are those that feature opposition or critical content run by individuals or organizations based in the country or the diaspora. The government's approach to internet filtering generally entails hindering access to a list of specific internet protocol (IP) addresses or domain names at the level of the EthioTelecom-controlled international gateway. Deep-packet inspection (DPI) is also employed, which blocks websites based on a keyword in the content of a website or piece of communication (such as email).

During the coverage period, over one hundred websites remained inaccessible in Ethiopia. Blocked websites

---

36 Test conducted by an anonymous researcher contracted by Freedom House, March 2015. During the test, some websites opened at the first attempt but were inaccessible when refreshed.
sites included Ethiopian news websites, political party websites, blogs, television and online radio websites, and the websites of international digital rights organizations, such as the Electronic Frontier Foundation and Tactical Technology Collective. Select tools such as text messaging apps and services on Google’s Android operating system on smartphones were inaccessible at irregular intervals but for unclear reasons.

Online censorship intensified as the country prepared for the May 2015 general elections, with new blocks on dozens of social media pages, blogs, and diaspora-based opposition websites that were created to report on the general election. A diaspora-operated website called AddisVoice, which published a series of critical articles about the educational qualifications of government officials, was a top target for blocking in 2014-2015. International news outlets were also targeted. In June 2014, the Ethiopian authorities were accused of jamming the satellite operations of the BBC, Deutsche Welle, France 24, and the Voice of America, blocking a few of the stations’ websites as well. Al Arabiya, a Saudi Arabia-based media outlet, and Al Jazeera’s Arabic and English websites were intermittently blocked throughout the coverage period.

Blogs are also a prime target for blocking. In 2007, the government instituted a blanket block on the domain names of two popular blog-hosting websites, Blogspot and Nazret, though the authorities have since become more sophisticated in their censorship techniques, now blocking select pages such as the Zone9 independent blog hosted on Blogspot, as opposed to the entire blogging platform. Nazret, however, remained completely blocked as of June 2015.

Facebook and Twitter platforms were otherwise generally accessible, although some individual Facebook groups belonging to opposition individuals remained blocked altogether when accessed via the unencrypted (HTTP) URL pathway. However, the social media curation tool Storify—first blocked in July 2012—remained blocked during the coverage period, in addition to the URL shortening tool Bit.ly. Circumvention tools are also blocked, including Tor—an online tool that enables users to browse anonymously—which has been blocked since May 2012. According to an independent source, key terms such as “proxy” yield no search results on unencrypted search engines, reflecting the government’s efforts to limit users’ access to circumvention tools and strategies.

Some restrictions are also placed on mobile phones, such as the requirement for a text message

---

37 Interview with the producer of a website called Mircha.org, http://mircha.org/category/english/
41 Zone9, blog post, October 8, 2015, http://zone9ethio.blogspot.com/.
47 A 2014 report from Human Rights Watch also noted that the term “aljazeera” was unsearchable on Google while the news site was blocked from August 2012 to mid-March 2013. According to HRW research, the keywords “OLF” and “ONLF” (acronyms of Ethiopian opposition groups) are not searchable on the unencrypted version of Google (http://) and other popular search engines. Human Rights Watch, “They Know Everything We Do,” March 25, 2014, 56, 58, http://bit.ly/1NViu6c.
Ethiopia

to obtain prior approval from EthioTelecom if it is to be sent to more than ten recipients.\textsuperscript{47} A bulk text message sent without prior approval is automatically blocked, irrespective of the content of the message.

There are no procedures for determining which websites are blocked or why, precluding any avenues for appeal. There are no published lists of blocked websites or publicly available criteria for how such decisions are made, and users are met with an error message when trying to access blocked content. This lack of transparency is exacerbated by the government’s continued denial of its censorship efforts. Meanwhile, the decision-making process does not appear to be controlled by a single entity, as various government bodies—including the Information Network Security Agency (INSA), EthioTelecom, and the ICT ministry—seem to be implementing their own lists, contributing to a phenomenon of inconsistent blocking. Government officials flatly deny the blocking of websites or jamming of international satellite operations while also stating that the government has a legal and a moral responsibility to protect the Ethiopian public from extremist content.

Content Removal

In addition to increasing blocks of online content, politically objectionable content is often targeted for removal, often by way of threats from security officials who personally seek out users and bloggers to instruct them to take down certain content, particularly critical content on Facebook. The growing practice suggests that at least some voices within Ethiopia’s small online community are being closely monitored. For instance, during the various legal proceedings of the Zone 9 bloggers throughout 2014-2015 (see “Prosecutions”), friends and reporters who posted pictures and stories of the trials on social media were briefly detained and asked to remove them.\textsuperscript{48}

Media, Diversity, and Content Manipulation

Lack of adequate funding is a significant challenge for independent online media in Ethiopia, as fear of government pressure dissuades local businesses from advertising with politically critical websites. A 2012 Advertising Proclamation also prohibits advertisements from firms “whose capital is shared by foreign nationals.”\textsuperscript{49} Launching a website on the local .et domain is expensive and onerous,\textsuperscript{50} requiring a business license from the Ministry of Trade and Industry and a permit from an authorized body.\textsuperscript{51} While the domestic Ethiopian blogosphere has been expanding, most blogs are hosted on international platforms by diaspora community members.

Despite extremely low levels of internet access, the authorities employ progovernment commentators and trolls to manipulate the online news and information landscape. There was a noticeable increase in the number of progovernment commentators in the last few years, as confirmed in a

\textsuperscript{47} Interview with individuals working in the telecom sector, as well as a test conducted by a Freedom House consultant who found it was not possible for an ordinary user to send out a bulk text message.

\textsuperscript{48} Reporters prevented from reporting on the trial of Zone9 Bloggers: Trial Tracker Blog, http://trialtrackerblog.org/home/.


\textsuperscript{51} Chala, “When blogging is held hostage of Ethiopia’s telecom policy.”
Ethiopia

June 2014 report by the Ethiopian Satellite Television Service (ESAT) that detailed the government’s efforts to recruit and train progovernment citizens to attack politically objectionable content online. According to the ESAT report, hundreds of bloggers reporting directly to government officials had been trained on how to post progovernment comments and criticize antigovernment articles on social media platforms.52

Meanwhile, increasing repression against journalists and bloggers has had a major chilling effect on expression online, particularly following the arrest of the Zone 9 bloggers in April 2014 and their ongoing trials throughout 2014-2015 (see “Prosecutions”). Fear of pervasive surveillance has also led to widespread self-censorship, and many bloggers publish anonymously to avoid reprisals.53 Local newspapers and web outlets receive their independent news and information from regime critics and opposition organizations in the diaspora, and few Ethiopian journalists work for either domestic print media or overseas online outlets due to the threat of repercussions.

Digital Activism

Despite very low internet penetration in the country, tech-savvy Ethiopians are increasingly using social media for campaigning and social activism. Digital activism was particularly pronounced and widespread following the arrest of six Zone 9 bloggers and three journalists for their alleged affiliation with the Zone 9 collective (see “Violations of User Rights”). Ethiopian bloggers and social media users flocked online to spread the #FreeZone9Bloggers hashtag in a campaign that quickly swept across the social media sphere and garnered widespread support from around the world throughout 2014-2015. In the first five days of the campaign, the #FreeZone9Bloggers hashtag was tweeted more than 8,000 times.54 While the international campaign elicited no official response from the government, sustained digital activism throughout the year continually informed the international community of the Zone 9 case, pushing high level diplomats to condemn the Ethiopian government’s actions, which many believe helped lead to the release of two of the bloggers in July 2015.

Following the prominence of the Zone 9 blogger campaign, hashtag campaigns on social media have become one of the most popular methods of activism in Ethiopia, enabling citizens to demand for social change and justice on a variety of issues. Two hashtag campaigns in late 2014 were particularly active on Ethiopian social media. One campaign, #BecauseIamOromo, stemmed from the release of an Amnesty International report on repression and human rights violations in the Oromo region of Ethiopia,55 building momentum across a three-day Twitter campaign, which attracted a significant number of followers.56 Another campaign, #Justice4Hanna, demanded justice for a 16 year old high school girl who was gang-raped and then later died from associated injuries in Addis Ababa in October 2014.57

Digital activism was also prominent in the lead-up to the May 2015 general elections, though calls

---

54 “#BBCtrending: Jailed bloggers spark Ethiopia trend,” BBC Trending, April 30, 2014, http://bbc.in/1kpaTDX.
for protest came mostly from the Ethiopian diaspora rather than from local activists who feared the government’s violent crackdowns against protest movements. State media stepped up its campaign against the press, in general, and the use of social media, in particular, claiming that foreign agents and terrorists were using social media to destabilize the country.

Violations of User Rights

The limited space for online expression continued to deteriorate alongside an increasing crackdown on bloggers. The Zone 9 bloggers arrested in April 2014 were charged with terrorism in July 2014 and subsequently subjected to a series of sham trials through mid-2015. In July 2015, two of the imprisoned Zone 9 bloggers were unexpectedly released and acquitted of all charges, leaving four in prison alongside five other individuals who were arrested in July 2014 and charged with terrorism for their various ICT activities. Independent journalists in the diaspora were targeted with Hacking Team surveillance spyware.

Legal Environment

The 1995 Ethiopian constitution guarantees freedom of expression, freedom of the press, and access to information, while also prohibiting censorship. These constitutional guarantees are affirmed in the 2008 Mass Media and Freedom of Information Proclamation, known as the press law, which governs the print media. Nevertheless, the press law also includes problematic provisions that contradict constitutional protections and restrict free expression, such as onerous registration processes for media outlets and high fines for defamation. The Criminal Code also penalizes defamation with a fine or up to one year in prison.

In 2012, the government introduced specific restrictions on an array of ICT activities under amendments to the 1996 Telecom Fraud Offences Law, which had already placed bans on certain communication applications, such as Voice over Internet Protocol (VoIP) like Skype and Google Voice, call back services, and internet-based fax services. Under the 2012 amendments, the penalties under the preexisting ban were toughened, increasing the fine and maximum prison sentence from five to eight years for service providers, and penalizing users with three months to two years in prison. The law also added the requirement for all individuals to register their telecommunications equip-

63 The government first instituted the ban on VoIP in 2002 after it gained popularity as a less expensive means of communication and began draining revenue from the traditional telephone business belonging to the state-owned Ethio Telecom. In response to widespread criticisms, the government claimed that VoIP applications such as Skype would not be considered under the new law, though the proclamation’s language still enables the authorities to interpret it broadly at whim.
65 A Proclamation on Telecom Fraud Offence.
Ethiopia

ment—including smartphones—with the government, which security officials typically enforce by confiscating ICT equipment when a registration permit cannot be furnished at security checkpoints, according to sources in the country.

Most alarmingly, the 2012 Telecom Fraud Offences Law extended the violations and penalties defined in the 2009 Anti-Terrorism Proclamation and criminal code to electronic communications, which explicitly include both mobile phone and internet services. The anti-terrorism legislation prescribes prison sentences of up to 20 years for the publication of statements that can be understood as a direct or indirect encouragement of terrorism, a vaguely defined term.

According to a December 2014 news report by Ethiopian State Television, a draft Computer and Internet Crime Bill is currently in the works by the Information Network Security Agency (INSA). The news report featured remarks by the INSA director, who insisted that the draft cybercrime law aimed to strengthen the government’s powers to prevent, control, investigate, and prosecute cybercrimes, including on social media. Observers are concerned that the law will empower state agencies to monitor private social media activities without oversight.

Prosecutions and Detentions for Online Activities

Ethiopia is among the world’s top five jailers of journalists. In 2014-2015, the authorities intensified their crackdown against bloggers and online journalists, using the country’s harsh laws to arrest and prosecute individuals for their online activities and silence dissent. Most alarmingly, six bloggers from the critical Zone 9 blogging collective and three journalists with alleged associations to Zone 9 were arrested in late April 2014. The arrests occurred just days following a Facebook post announcing the group’s plans to resume its activism after taking a seven-month hiatus due to “a considerable amount of surveillance and harassment” the bloggers had previously suffered at the hands of security agents for their writings and social media activism.

Initially held for three months without charges, the bloggers were charged in July 2014 with terrorism under the harsh Anti-Terrorism Proclamation for conspiring with the banned opposition group Ginbot 7, which the government classifies as a terrorist group. The bloggers were further accused of encrypting their communications to disseminate seditious writings with the intent of overthrowing the government, the latter of which is an offense under the criminal code. The government reportedly submitted 30 pages of phone and surveillance records spanning a period of three

71 “Federal High Court Lideta Criminal Bench court, Addis Ababa,” http://1drv.ms/1OqAjlC.
years as evidence of the terrorism charges, alongside email communications and digital security handbooks.

Despite widespread international condemnation of the Zone 9 arrests, the detainees were denied bail and brought to court dozens of times without any progress to their case for more than a year. During the trials between June and November 2014, at least three other individuals were arrested temporarily for posting updates and pictures of their trials on social media via mobile devices.

Several other critical bloggers and online activists were arrested in July 2014, including Abraha Desta and Zelalem Workagegnehu, both academics and bloggers who were held without charges for four months until October 2014 when they were charged for their alleged support of the opposition group Ginbot 7. They were also charged with using social media to contact members of Ginbot 7. Widely known for his Facebook posts criticizing the ruling party, Abraha Desta was reportedly beaten brutally before being taken to an unidentified prison. Three other individuals—Yonatan Wolde, Abraham Solomon, and Bahiru Degu—were also arrested around the same time for allegedly applying for an internet security and social media training abroad. At a court hearing in August 2015, the defendants’ cases were delayed until November.

Meanwhile, the well-known dissident journalist and blogger Eskinder Nega is still carrying out an 18-year prison sentence handed down in July 2012 under the anti-terrorism law.

**Surveillance and Anonymity**

Government surveillance of online and mobile phone communications is pervasive in Ethiopia, and evidence has emerged in recent years that reveal the scale of such practices. According to 2014 Human Rights Watch research, there are strong indications that the government has deployed a
Ethiopia

centralized monitoring system from the Chinese telecommunications firm ZTE, known as ZXMT, to monitor phone lines and various types of communications, including mobile phone networks and the internet. Known for its use by repressive regimes in Libya and Iran, ZXMT enables deep packet inspection (DPI) of internet traffic across the EthioTelecom network and has the ability to intercept emails and web chats.

Another ZTE technology, known as ZSmart, is a customer management database installed at EthioTelecom that provides the government with full access to user information and the ability to intercept SMS text messages and record phone conversations. ZSmart also allows security officials to locate targeted individuals through real-time geolocation tracking of mobile phones. While the extent to which the government has made use of the full range of ZTE’s sophisticated surveillance systems is unclear, the authorities frequently present intercepted emails and phone calls as evidence during trials against journalists and bloggers or during interrogations as a scare tactic.

There has been an increasing trend of exiled dissidents targeted with surveillance malware in the past few years (see “Technical Attacks”). Recent Citizen Lab research published in March 2015 uncovered the use of Remote Control System (RCS) spyware against two employees of the diaspora-run independent satellite television, radio, and online news media outlet, Ethiopian Satellite Television Service (ESAT), based in Alexandria, Virginia, in November and December 2014. Made by the Italian company Hacking Team, RCS spyware is advertised as “offensive technology” sold exclusively to law enforcement and intelligence agencies around the world, and has the ability to steal files and passwords, as well as to intercept Skype calls and chats.

While Hacking Team claims that they do not deal with “repressive regimes,” the social engineering tactics used to bait the two ESAT employees made it clear that the attack was targeted. Moreover, analysis of the RCS attacks uncovered credible links to the Ethiopian government, with the spyware’s servers registered at an EthioTelecom address under the name “INSA-PC,” referring to the Information Network Security Agency (INSA), the body established in 2011 to preside over the security of the country’s critical communications infrastructure. INSA was already known to be using the commercial toolkit FinFisher—a device that can secretly monitor computers by turning on webcams, record everything a user types with a key logger, and intercept Skype calls—to target dissidents and supposed national security threats.

Given the high degree of online repression in Ethiopia, political commentators use proxy servers and anonymizing tools to hide their identities when publishing online and to circumvent filtering, though

---

83 Human Rights Watch, “They Know Everything We Do,” 62.
84 Human Rights Watch, “They Know Everything We Do,” 67.
85 Ibid, 52.
90 Marczak et al., Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware.
Ethiopia

the ability to communicate anonymously has become more difficult. The Tor Network anonymizing tool has been blocked since May 2012.

Anonymity is further compromised by strict SIM card registration requirements. Upon purchase of a SIM card through EthioTelecom or an authorized reseller, individuals must provide their full name, address, government-issued identification number, and a passport-sized photograph. EthioTelecom's database of SIM registrants enables the government to cut-off the SIM cards belonging to targeted individuals and to restrict those individuals from registering for new SIM cards. Internet subscribers are also required to register their personal details, including their home address, with the government. In 2013, an inside informant leaked worrying details of potential draft legislation that seeks to mandate real-name registration for all internet users in Ethiopia, though there are no further details of this development as of mid-2015.92

While the government's stronghold over the Ethiopian ICT sector enables it to proactively monitor users, its access to user activity and information is less direct at cybercafes. For a period following the 2005 elections, cybercafe owners were required to keep a register of their clients, but the requirement has not been enforced since mid-2010.93 Nevertheless, some cybercafe operators revealed that they are required to report any "unusual behavior" to security officials, and officials often visit cybercafes (sometimes in plainclothes) to ask questions about specific users or to monitor user activity themselves.94

Intimidation and Violence

Government security agents frequently harass and intimidate bloggers, online journalists, and ordinary users for their online activities. Independent bloggers are often summoned by the authorities to be warned against discussing certain topics online, while activists claim that they are consistently threatened by state security agents for their online activism.95 Prior to their imprisonment in April 2014, the Zone 9 bloggers reported suffering a considerable amount of harassment for their work, leading them to go silent for several months. Shortly after the bloggers announced a resumption of activities on Facebook in April 2014, six Zone 9 bloggers were arrested and sent to a federal detention center in Addis Ababa where they were reportedly mistreated and tortured to give false confessions throughout the year.96 The active Gmail accounts belonging to several of the Zone 9 bloggers while in detention suggests that they may have been forced give their passwords to security officials against their will.97

Ethiopian journalists in the diaspora have also been targeted for harassment, according to one

---

92 Interview conducted by Freedom House consultant.
94 Human Rights Watch, “They Know Everything We Do,” 67.
96 Trial Tracker Blog, “Trials.”
97 Anonymous Freedom House researcher reported seeing several of the detained Zone9 bloggers actively online in Gmail chat.
Ethiopia

reporter of the diaspora-based website ECADF, who received death threats from an alleged government spy in Netherlands for his reporting.98

Technical Attacks

Opposition critics and independent voices face frequent technical attacks, even when based abroad. In recent years, independent research has found evidence that the Ethiopian authorities use sophisticated surveillance malware and spyware, such as FinFisher’s FinSpy and Hacking Team’s Remote Control Servers (RCS), to target exiled dissidents. The most recent attack was recorded in December 2014 by researchers at Citizen Lab, who discovered RCS spyware in attached documents sent in emails to journalists with the Ethiopian Satellite Television Service (ESAT), an independent TV, radio, and online news outlet run by members of the Ethiopian diaspora in Virginia.99 Having been targeted with the RCS spyware before,100 the journalists did not download the attachments that would have installed the spyware and enabled the attackers to access files on the infected computers. The journalists believe the attack was an effort by the authorities to ascertain ESAT’s sources within Ethiopia.

Meanwhile, a technical attack in late 2012 and early 2013 on an exiled dissident (and American citizen) is currently the basis of an ongoing legal case at a U.S. District Court filed by the Electronic Frontier Foundation (EFF).101 In April 2013, EFF sued the Ethiopian government in a U.S. court on behalf of the anonymous Ethiopian dissident for implanting malicious FinSpy malware on the individual’s computer. Linked to a server belonging to EthioTelecom, FinSpy had secretly recorded dozens of Skype calls, copied emails the individual had sent, and logged a web search conducted by his son on the history of sports medicine for a school research project.102

99 Marczak et al., Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware.
France

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>13</td>
<td>15</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>20</td>
<td>24</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

**Key Developments: June 2014 – May 2015**

- Two decrees were issued in early 2015 outlining administrative measures for the blocking and de-indexing of websites for terrorist content. The decrees earned the ire of free speech advocates as the blacklist of websites is compiled by a police agency without court approval (see **Blocking and Filtering** and **Content Removal**).

- An antiterrorism law passed in November 2014 outlined harsh prison sentences for the broad offense of “apology for terrorism” through online speech (see **Legal Environment**), leading to several users being arrested, and some imprisoned, for online comments that were seen as condoning the January 2015 terrorist attacks that targeted the offices of satirical magazine *Charlie Hebdo* (see **Prosecutions and Detentions**).

- Surveillance powers were bolstered after the *Charlie Hebdo* attacks with the passage of a new law in May 2015 requiring internet service providers to install devices to monitor users’ “suspicious behavior” and provide unfettered access to intelligence agencies (see **Surveillance, Privacy, and Anonymity**).

- French broadcaster TV5Monde was hit by a massive cyberattack in April 2015 by Islamist hackers calling themselves the “CyberCaliphate.” Eleven channels were brought offline for a day (see **Technical Attacks**).
France

Introduction

France was rocked by a series of terrorist attacks in January 2015 in which 12 people were shot and killed by armed extremists, including eight staff at the controversial French satirical magazine *Charlie Hebdo*. The attacks attracted global solidarity under the slogan “Je suis Charlie” (I am Charlie), and an estimated 3.7 million marched in the streets of France in support of free speech.\(^1\) Reacting to the incidents, French law enforcement agencies took a heavy handed approach by arresting dozens for apologie du terrorisme (apology for terrorism), an offense dating from the 19th century and updated only two months before the attacks to include online offenses.

The government, too, went into overdrive. Prime Minister Manuel Valls issued two decrees outlining administrative measures for the blocking and de-indexing of terrorist content without the need for a court order. In May, legislators passed a new surveillance law granting intelligence agencies the power to intercept electronic communications in real time and request the immediate handover of user data from ISPs, also without the need for prior court approval. A similar law had been passed in December 2013, granting extended legal powers for authorities to gain access to or record telephone conversations, emails, internet activity, personal location data and other electronic communications for a broad range of purposes, including “national security,” the protection of France’s “scientific and economical potential,” and prevention of “terrorism” or “criminality.”

While France has traditionally maintained a relatively open and accessible internet, several actions on the part of successive administrations have raised concerns from internet freedom groups and free speech activists. Politicians have proposed highly restrictive measures such as the imprisonment of frequent visitors to extremist websites, the mandatory registration of online news editors,\(^2\) a bandwidth tax, and the banning of the online sale of goods below market prices.\(^3\) More significantly, France’s data protection agency has intensified its legal battle against Google regarding the controversial “right to be forgotten.” While Google has begun to cooperate with authorities in European Union (EU) countries since a major ruling of the EU Court of Justice in May 2014, the company has been blamed by the French authorities for only applying the ruling on European versions of the search engine’s site. The back-and-forth has launched a debate about the extraterritorial application of national laws.

Obstacles to Access

*France has a highly developed telecommunications infrastructure and a history of innovation in information and communications technologies (ICTs).*\(^4\) Starting in the 1970s, France began developing Teletex and Videotex technologies, leading to the introduction of the widely popular Videotex service Minitel in 1982, which was accessible through telephone lines. In many ways, Minitel predicted applications of the modern internet, such as travel reservations, online retail, mail, chat, and news. At its peak, Minitel had around nine million users, and hundreds of thousands continued to use the service, even

---


after the World Wide Web was introduced in 1994. It was not until June 2012 that the Minitel service was discontinued, primarily due to the growth of the internet industry. France's current ICT market is open, highly competitive, and has benefitted from the privatization of the state-owned company France Telecom.

Availability and Ease of Access

The French government has been committed to providing widespread access to high-speed broadband and has promised to achieve universal coverage by 2025. As a part of this plan, in February 2013 Alcatel-Lucent and Orange (France Telecom) announced the deployment of the world's most powerful broadband infrastructure, an optical-link, 400 Gbps line between Paris and Lyon. In April 2015, the French parliament approved an amendment to the telecoms component of France's economic reform law, known as the Loi Macron, requiring telecom operators to improve mobile coverage throughout the country. The law will ensure that residents of an estimated 170 municipalities, which currently have no access to mobile services, will be covered by mobile networks by 2017. Failure to comply with the obligations can result in sanctions from the telecoms regulator.

France had an internet penetration rate of 83.75 percent at the end of 2014, up from 71.58 percent five years earlier. Fixed broadband use increased during the same period, from 31.57 percent to 40.18 percent. Regionally, penetration ranges from 84.4 percent in the Paris area to 65 percent in the northwest of France. Most at-home users have access to broadband connections, while the remaining households are connected either through dial-up or satellite services, usually due to their rural location. Over 5 million households did not use the internet in 2014, either due to obstacles to access, or personal choice. As French statisticians do not record information related to race, there is no government data relating to internet use according to ethnicity. On a positive note, there is little or no gender gap when it comes to internet access.

---

France

The average monthly cost of broadband internet access in France is approximately EUR 30 (US$ 43), for both ADSL\(^{17}\) and fiber-optic connections.\(^{18}\) Considering the average monthly income is EUR 2,359 (US$ 3,279),\(^{19}\) this makes internet access fairly affordable for a large percentage of the population. The average household net-adjusted disposable income per capita is EUR 25,308 a year, more than the OECD average of EUR 23,298 a year; however, there is a considerable gap between the richest and poorest.\(^{20}\) Companies such as Free Telecom offer cheap internet access and mobile contracts through bundled deals. Akamai data indicates that, in terms of the global average, France saw a 0.1 percent drop in internet speeds to 6.6bpms in the first quarter of 2014.\(^{21}\)

There were 64.875 million mobile contracts in use in France at the end of 2014, representing a penetration rate of over 100 percent.\(^{22}\) Over 23 million people use their mobile devices to access the internet,\(^{23}\) mostly in addition to a household connection.\(^{24}\)

Restrictions on Connectivity

There were no restrictions on connectivity reported over the past year. There is no central internet backbone and ISPs are not required to lease bandwidth from a monopoly holder. Instead, the backbone consists of several interconnected networks run by ISPs and shared through peering or transit agreements. There are also a number of Internet Exchange Points (IXPs) in France,\(^{25}\) which contribute to improved access and lower consumer prices.\(^{26}\)

Network and internet service providers are usually prohibited from discrimination and favoritism on the principal of net neutrality, but some incidents in recent years have concerned digital rights activists. The French Competition Authority (FCA) issued a decision on September 20, 2012 regarding the conflict between the U.S. operator Cogent and the French company Orange on whether network operators are allowed to charge for opening additional capacity. The FCA considered that such an action was not liable to contravene competition law inasmuch as Orange did not refuse access to its subscribers from Cogent, but asked for repayment for opening new capacity in accordance with its peering policy.

Furthermore, Culture Minister Fleur Pellerin has stated her desire to introduce a new tax on the “use of bandwidth.”\(^{27}\) In January 2015, the minister said she wanted a “level playing field” for French

---


\(^{21}\) Akamai’s State of the Internet Q1 2014 Report; Volume 7 Number 1; Section 3 Geography – Global, accessed May 21 2015 http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf


\(^{25}\) Internet Exchange Points, Data Centre Map, accessed May 22 2015 http://www.datacentermap.com/ixps.html

\(^{26}\) “Internet Service Providers and Peering v3.0,” accessed May 22 2015 http://www.drpeering.net/white-papers/Internet-Service-Providers-And-Peering.html

ICT Market

There are no significant business hurdles to providing access to digital technologies in France. The main ISPs are Orange, Free, SFR, Bouygues Telecom, and Numericable, with around 40 smaller private and non-profit ISPs. Apart from Numericable, these ISPs are also the four main mobile phone operators and work in conjunction with some 40 mobile virtual network operators (MVNOs). The government owns a total of 27 percent of shares in Orange, which was formerly a state-owned company under the name France Telecom, through direct ownership as well as holdings in its sovereign wealth fund. Another provider, Free, has quickly picked up market share since launching 3G services in 2009 through aggressive pricing practices. This price war led the French media conglomerate Vivendi to sell its mobile phone company SFR; in April 2014, Vivendi accepted a EUR 17 billion (US$22.85 billion) offer from Numericable. In the meantime, Bouygues Telecom has begun a round of strategic downsizing after failing to sell its assets.

Regulatory Bodies

The telecommunications industry in France is regulated by the Regulatory Authority for Electronic and Postal Communication (ARCEP), while competition is regulated by France’s Competition Authority and, more broadly, by the European Commission (EC). The commissioner of ARCEP is appointed by the government, though as an EU member state, France must ensure the independence of its national telecommunications regulator. Given that the French state is a shareholder in Orange, the country’s leading telecommunications company, the EC stated that it would closely monitor the situation in France to ensure that European regulations were being met. The EC has previously stepped in when the independence of national telecommunications regulators seemed under threat, notably in Romania, Latvia, Lithuania, and Slovenia. ARCEP remains an independent and impartial body and decisions made by the regulator are usually seen as fair.

---

29 According to Cofisem, as of July 2013, the major shareholders in Orange were Fonds Stratégique d’Investissement (13.5%), French State (13.45%), Employees (4.81%), and company-owned shares (0.58%). 67.66% are owned by “other shareholders.” “Orange – European Equities,” NYSE Euronext, accessed March 16 2014, https://europa.nequities.nyse.com/en/products/equities/FR0000133308-XPAR/company-information.  
France

In the past, ARCEP has taken decisions to ensure the fairness of the telecommunications market. ARCEP placed Free under investigation in early 2013 after the ISP released a firmware update that included an “ad-blocker” function to remove advertisements from appearing on websites. Executives at Free were reportedly attempting to force Google to compensate the ISP for the high levels of data traffic coming from YouTube and other Google sites. The American company had made a similar agreement with leading ISP Orange. Free backed down under government pressure and criticism that the ISP was harming net neutrality by failing to deliver unobstructed content.

Limits on Content

Two decrees related to blocking and de-indexing websites from search engine results without a court order were issued in the wake of the Charlie Hebdo attacks. President Hollande stated his desire to introduce measures to hold internet companies responsible for any pro-terrorist material published on their sites. Social media was used to organize massive protests in defense of free speech.

Blocking and Filtering

France does not generally engage in any politically motivated blocking of websites. YouTube, Facebook, Twitter and international blog-hosting services as a whole are freely available. In December 2014, French ISPs were ordered to block dozens of URLs that grant access to the popular file-sharing website The Pirate Bay. Some observers expect that future blocks on websites that are used to access copyrighted materials may be in store.

Many have feared that that laws such as the Law for Confidence in the Digital Economy (LCEN), the Law on Guidelines and Programming for the Performance of Internal Security (LOPPSI 2), and that establishing the High Authority on the Defense of Intellectual Property (known as the HADOPI law) may eventually lead to a spillover whereby controversial yet legal sites are censored by administrative agencies without a court order. This scenario unfolded over the past year, with the issuance of a decree by the prime minister in February 2015.

The decree implements article 6-1 of LCEN, passed in 2004, as well as article 12 of new antiterrorism law passed in November 2014. The article calls for the Central Office for the Fight against Crime related to Information and Communication Technology (OCLCTIC) to create a blacklist of sites contain-

40 Loi d’orientation et de programmation pour la performance de la sécurité intérieure.
ing materials that incite or condone terrorism, as well as sites that display child pornography, and to review the list every four months to ensure that blacklisted sites continue to contravene French law. ISPs must then take all appropriate measures to restrict access to those sites within 24 hours of notification. Users trying to access those pages are redirected to a website from the Ministry of Interior indicating why the site was blocked and avenues for appeal. The blacklist is also shared with the head of the National Commission on Informatics and Liberty (CNIL), who may appeal decisions taken by the OCLCTIC.

UberPop, a ride-sharing and ride-hailing app created by the American company Uber, was banned in January 2015. Earlier, a court had refused to ban the app, triggering massive strikes by French taxi drivers that brought traffic to a standstill in the capital Paris. The strikes led the government to pass a new law tightening regulations on the taxi and chauffeur industry that effectively banned UberPop drivers without a professional license. The law was challenged in the Constitutional Court and upheld in September 2015. UberPop services were halted by the company in July 2015.

Content Removal

French authorities are fairly transparent about what content is prohibited and the reasons behind specific content removal requests. Incitement of hatred, racism, Holocaust denial, child pornography, copyright infringement, and defamation are illegal. Article R645-1 of the French criminal code outlaws the display of the emblems, uniforms, or badges of criminal organizations, under penalty of a fine. Websites that contravene this law are requested to remove the content or face blocking.

Over the past year, search engines have come under particular pressure regarding issues of terrorism, child pornography, and privacy. On March 4, 2015, a government decree was issued relating to the de-indexing of sites that incite terrorism or apologize for terrorism, as well as sites that display child pornography, from search engine results. The decree implements modifications to the 2004 LCEN that were made under the 2011 LOPPSI 2 and 2014 antiterrorism law, allowing for the de-indexing of online content using an entirely administrative procedure. The decree on de-indexing states that OCLCTIC will transfer demands to search engines companies, who then have 48 hours to comply. The OCLCTIC is responsible for reevaluating de-indexed websites every four months, and requesting the relisting of websites where the incriminating content has been removed. The procedure is supervised by the CNIL. President François Hollande said the law would hold tech companies as

“accomplices” to terrorism should they fail to act.\textsuperscript{51} The process has been criticized as lacking judicial oversight.

The legal debate over the right to be forgotten has also escalated over the past year. On May 13, 2014, the Court of Justice of the European Union (CJEU) found that the 1995 Data Protection Directive applies to the activities of search engines like Google, and requires companies to remove certain search results if the data is deemed to violate an individual’s right to privacy.\textsuperscript{52} The court decided that by searching automatically, constantly, and systematically for information on the internet, search engines are “collecting” and “processing” data within the meaning of the directive. Based on this ruling, individuals within the European Union can now request that search engines remove links associated with their name, but only in searches for that individual’s name and under the condition that the information in the links is “inadequate, irrelevant, or no longer relevant” and is not considered to be in the public interest. Many critics of this ruling argued that the court should not have granted private companies the authority to arbitrate competing concerns between the right to privacy and the right to information, and that the court failed to establish clear guidelines regarding when links to data should be removed.\textsuperscript{53}

Since the ruling, Google has received over 68,000 requests from French users to remove almost 230,000 URLs. France has the highest number of requests out of any country in the European Union, accounting for around 20 percent of all requests. Google states in its latest transparency report that 51.7 percent of those URLs have been removed from search results when appearing on the local site of the Google search engine, for example, Google.fr.\textsuperscript{54} In June 2015, CNIL, France’s data protection authority, ordered Google to extend its right to be forgotten across all of its local sites, including Google.com.\textsuperscript{55} The order was rejected by Google on concerns the move would set a dangerous precedent for authoritarian governments, who could also request that Google apply unjust national laws extraterritorially, thus altering the web experience for all.\textsuperscript{56} An informal appeal by Google was rejected by CNIL in September 2015.\textsuperscript{57}

Media, Diversity, and Content Manipulation

France is home to a highly diverse online media environment. Self-censorship online is minimal and there were no reports of the French government proactively manipulating online content.

\textsuperscript{56} Peter Fleischer, “Implementing a European, not global, right to be forgotten,” Google Policy Europe blog, July 30, 2015, http://googlepolicieurope.blogspot.co.uk/2015/07/implementing-european-not-global-right.html.
Digital Activism

French digital rights and advocacy groups are very active in the country, playing a significant role in protesting the government’s recent moves to expand blocking and surveillance without judicial oversight. The Association of Community-based Internet Services (ASIC) and La Quadrature du Net have stated their intention to appeal to the Council of State in order to overturn these decrees that limit online freedoms. 58 The latter created the website Presumed Terrorists to inform French citizens and advocate against the law’s passage. 59 In the past, La Quadrature du Net successfully lobbied the European Parliament for an amendment to the European Union Telecoms Package to ensure that no restrictions on internet access could be imposed without prior judicial approval. 60

The hashtag #jesuischarlie gained worldwide prominence in the wake of the attacks on Charlie Hebdo to express support for free speech and support for those killed. Around two million people took to the streets in Paris and four million throughout the country in coordinated marches. 61

Violations of User Rights

Both in the lead up and reaction to terrorist attacks in Paris, the French government introduced several new measures that threaten internet freedom in the country. A new antiterrorism law was passed in November 2014 that introduced penalties for online speech that is deemed to “apologize for terrorism.” Following the January 2015 shootings, there were renewed calls to expand state surveillance of electronic communications, culminating in the passage of a new surveillance law in May. The law granted intelligence agencies the power to intercept electronic communications in real time and request the immediate handover of user data from ISPs, without the need for prior court approval.

Legal Environment

France’s constitution guarantees freedom of speech, 62 in accordance with the 1789 Declaration of the Rights of Man. 63 The European Convention on Human Rights, of which France is a signatory, provides for freedom of expression, subject to certain restrictions which are “necessary in a democratic society.” 64 However, the French government has enacted several laws which, while seeking to protect the rights of internet users and copyright holders, also threaten the rights of citizens online. Several laws have been highlighted by online activists and internet companies over concerns that they may overreach in their aims. Electronic surveillance also operates under a vague legal framework, with some fears that intelligence authorities have engaged in extralegal monitoring of users’ online ac-

63 “The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by law,” Declaration of the Rights of Man, 17 89, accessed March 17, 2014, http://avalon.law.yale.edu/18th_century/rightsof.asp.
France

activities and have cooperated with their transatlantic counterparts in the United States and United Kingdom.

An antiterrorism law was passed in November 2014 establishing that online speech deemed as "apology for terrorism" (apologie du terrorisme) can be punished by five years in prison and a EUR 75,000 (US$82,000) fine. The law also allowed for the blocking of terrorist websites (see "Blocking and Filtering").

In July 2013, following changes to the HADOPI laws on copyright, the government halted the practice of suspending users' internet access and reduced the set of fines incurred for repeated copyright violations. More than one year later, in October 2014, digital rights advocates raised concerns when Minister of Culture Fleur Pellerin proposed a new mandate for the organization entrusted with enforcing HADOPI, namely the blocking of copyright infringing websites according to a blacklist determined not by a court, but an administrative agency.

Prosecutions and Detentions for Online Activities

In the aftermath of the attacks on Charlie Hebdo, authorities cracked down on speech deemed apology for terrorism both offline and online.

- In Nantes, a 16-year-old was arrested for sharing an ironic cartoon on Facebook related to the Charlie Hebdo attack. The cartoon in question mocked the cover of the July 2013 issue of Charlie Hebdo, published after the massacre of hundreds of Egyptians protesting the coup against the Islamist former president Mohamed Morsi, which depicted a Muslim man who is holding a Koran in front of himself to defend against bullets is nevertheless shot stating, “It doesn’t stop bullets.” The cartoon in question, believed to be by the artist Dedko, replaced the Koran with Charlie Hebdo magazine and the man in Muslim garb with a staff cartoonist. Some complained of double-standards when it comes to the upholding of free speech by French authorities.

- In a case that attracted international attention, comedian Dieudonné M’bala M’bala was convicted of apologizing for terrorism and given a two-month suspended sentence in March 2015. He had been arrested in January over a Facebook post in which he stated, in French, “Tonight, as far as I am concerned, I feel like Charlie Coulibaly,” combining the popular “Je Suis Charlie” slogan with the name of Amedy Coulibaly, one of the attackers. Dieudonné argued that instead of being celebrated for free speech like the staff of...
Charlie Hebdo, he had been vilified by the media as if he was a terrorist like Coulibaly. The controversial comedian has been convicted of anti-Semitism and slander on seven previous occasions.

- In Strasbourg, a 30-year-old was arrested for posting “Bons baisers de Syrie – Bye bye Charlie” (From Syria with Love – Bye bye Charlie) on Facebook along with a photo of an AK-47.

- In Nantes, a 22-year old was convicted of 12 months in prison for a video published on Facebook in which he made fun of the death of Ahmed Merabet, a police officer killed during the attack on Charlie Hebdo.

- In Toulon, a 27-year-old was convicted of 3 to 12 months in prison for publishing jihadist photos and posts condoning the attack. He posted the following on Facebook in French: “We hit them good, put on your djellaba guys, we’ll never give up, there are other brothers in Marseille.”

Surveillance, Privacy, and Anonymity

Surveillance has escalated in recent years, not least with the passage of a new surveillance law in May 2015, which was passed in the wake of the attacks on Charlie Hebdo by armed extremists earlier that year. The Loi Relatif au Renseignement, or Intelligence Law, allows for intelligence agencies to conduct electronic surveillance without a court order and requires ISPs to install so-called “black boxes,” algorithms that analyze users’ metadata for “suspicious” behavior in real time. The law also provided a legal basis for the installation of recording devices in private homes as well as computer intrusion software such as keystroke logging software. Authorities can store the recordings for one month and metadata for five years. France’s prime minister, Manuel Valls, justified the new law as necessary given that the previous wiretapping law dated from 1991. The law was reviewed by the Constitutional Court and came into effect in July 2015. Mozilla and a group of ICT companies complained that the law “threatens the integrity of internet infrastructure, user privacy, and data security.” Reporters Without Borders called on the French Parliament to closely scrutinize the bill to ensure its compliance with international human rights law.
France

The Intelligence Law came after the passage of new regulations on electronic surveillance, which were passed in December 2013 and entered into force in January 2015, as part of a routine military spending bill (the Military Programming Law, or LPM). Article 20 of the LPM significantly expanded electronic surveillance of French residents and businesses by requiring ISPs to hand over data such as phone conversations, emails, internet activity, personal location data, and other electronic communication data to public authorities. The powers relate to the General Directorate for Internal Security (DCRI), to three intelligence agencies under the Ministry of Defense, as well as to anti-money-laundering and customs agencies. Under the law, these agencies can conduct surveillance without prior court approval for purposes of “national security,” the protection of France’s “scientific and economical potential,” and the prevention of “terrorism” or “criminality.”

The office of the prime minister authorizes surveillance and the National Commission for Security Interception (Commission nationale de contrôle des interceptions de sécurité, CNCIS) must be informed within 48 hours in order to ensure its approval. Critics have pointed out that the CNCIS lacks appropriate control mechanisms and independence from political interference, given that the CNCIS is composed of only three politicians. On the other hand, the government argued that the law provides an improved legal framework for practices that have already been in place for years.

Article 23 of LOPPSI 2, adopted in 2011, grants the police with the authority to install malware—such as keystroke logging software and Trojan horses—on a suspect’s computer in the course of counter-terrorism investigations, although authorization must come from a court order.

Intimidation and Violence

Online hate speech has been a topic of concern in France. Twitter has teamed up with SOS Homophobie, an LGBT rights NGO, to allow the charity to quickly and easily report homophobic tweets to the company’s staff. There were 2,197 instances of anti-LGBT speech reported to the organization in 2014, a steady increase over the years but a steep drop from 2013, when the partnership with Twitter began. Forty percent of all reported incidents occurred on the internet. Hashtags such as “#brûlonslesgayssurdu” (“let’s burn the gays on”) and “#lesgaysdoiventdisparaîtrecar” (“gays must die because”) have been trending, leading to three users being fined EUR 300-500 (US$330-550) for homophobic tweets in January 2015.

---

France

Technical Attacks

One of the main cybersecurity headlines over the past year in France was the hacking of the television and online news outlet TV5Monde on April 8, 2015. Hackers claiming to belong to the Islamic State breached the company’s information systems, overriding TV5Monde’s broadcasted programming for more than three hours and disabling live broadcasts for a day on 11 channels. The group, which called itself “CyberCaliphate,” also hacked the news company’s website and social media accounts.88 The Twitter account of French newspaper *Le Monde* was also hacked by supporters of the Syrian government in January 2015. In the weeks after the terrorist attacks against *Charlie Hebdo*, authorities reported some 19,000 cyberattacks against French websites.89

---

Gambia

Key Developments: June 2014 – May 2015

- Sporadic internet blackouts ensued throughout 2014 and 2015, which included a week-long outage in April 2015 (see Restrictions on Connectivity).
- While the popular Voice over Internet Protocol (VoIP) platform Viber was unblocked in July 2014, dozens of opposition and news websites remained blocked (see Blocking and Filtering).
- Anecdotal reports indicated an increasing trend of politically sensitive content “disappearing” from the internet due to intimidation from government authorities (see Content Removal).
- Digital activism led to the release of an activist and blogger, who was detained without charges for his work with the survey research firm, Gallup (see Digital Activism).
- In July 2014, a supporter of the main opposition party was prosecuted and fined US$1,250 for using Skype to send live coverage of an opposition political rally to the Freedom Newspaper online outlet based abroad (see Prosecutions and Detentions for Online Activities).
- A former online journalist was arrested in August 2014 on accusations of sending sensitive information to “enemies” of the government based abroad. Tortured while in detention, he was released without charges and subsequently fled the country. Extralegal detention and harassment led at least two other online journalists to flee the country in exile (see Prosecutions and Detentions for Online Activities and Intimidation and Violence).
Gambia

Introduction

Under the repressive rule of President Yahya Jammeh, who has been in power since overseeing a military coup in 1994, political rights and civil liberties are severely restricted in The Gambia, with conditions for press freedom and freedom of expression particularly tenuous. As access to information via information and communication technologies (ICTs) has proliferated over the past two decades, the government has proactively applied its notably harsh media censorship tactics to the internet, beginning as early as 2006 with the blocking of two critical online news outlets.1

In the past few years, the growing popularity of independent online news outlets, most of which are based abroad and operated by exiled Gambian journalists, has prompted the government to intensify its crackdown against critical voices by blocking dozens of news and opposition websites and arresting individuals suspected of disseminating information to exiled journalists. In 2014 and 2015, at least 20 news and opposition websites were blocked, while anecdotal reports indicated an increasing trend of politically sensitive content “disappearing” from the internet due to intimidation from government authorities. The popular Voice over IP (VoIP) platform, Viber, was blocked from March to July 2014.

Meanwhile, access to the internet was hampered by frequent internet blackouts lasting several hours throughout the coverage period. In April 2015, internet service was shut down completely for one week, which providers blamed on technical issues with the ACE submarine communications cable, though some local observers believed the disruptions were a result of the government’s increasing efforts to test new ways and means of controlling access to the internet and critical content.

Arrests, extralegal detentions, and threats against online journalists were common in 2014 and 2015, resulting in a growing number of online journalists fleeing the country in exile. In July 2014, an opposition supporter, Lansana Jobarteh, was prosecuted for allegedly broadcasting an opposition political rally in December 2013 without a license. Jobarteh was using Skype on his iPad to transmit coverage of the rally to the Freedom Newspaper online outlet based abroad. He was found guilty under restrictive ICT-specific amendments to the 2009 Information and Communications Act enacted in 2013 and sentenced to one year in prison or a fine of GMD 50,000 (about US$1,250), the latter of which was paid with support from members of his opposition party. The government unblocked Viber shortly after Jobarteh’s conviction. According to local legal experts, the timing of the two incidents suggests that the government may be shifting its restrictions on internet freedom away from blocking certain ICT tools and in favor of using restrictive legal measures to punish “perceived” enemies of the state.2

Obstacles to Access

Internet blackouts plagued The Gambia throughout the coverage period, lasting several hours at a time. A week-long shutdown occurred in April 2015, which providers blamed on technical issues, while local observers pointed to the government’s increasing efforts to test new ways and means of controlling access to the internet and critical content.

2 Interview with a human rights lawyer, on the condition of anonymity, February 2015.
Gambia

Availability and Ease of Access

Access to the internet in The Gambia has increased steadily over the past decade, from a penetration rate of less than 4 percent in 2004 to 16 percent in 2014, according to the latest data from the International Telecommunication Union (ITU).\(^3\) Fixed-broadband subscriptions were still paltry, however, at a penetration rate of a mere 0.12 percent in 2014 (increasing from 0.02 in 2013).\(^4\) By contrast, The Gambia has one of the highest mobile phone penetrations in Africa, with an access rate of 120 percent in 2014, up from nearly 100 percent in 2013,\(^5\) though only 1.2 percent of the population has access to mobile broadband.\(^6\) Nonetheless, connection speeds were very slow during the year, averaging 1.6 Mbps (compared to a global average of 4.5 Mbps), according to May 2015 data from Akamai’s “State of the Internet” report.\(^7\)

At a cost of about US$10 per month, fixed-line subscriptions are expensive for individual users in The Gambia, where average monthly household incomes are less than US$50 as of the latest available data from 2011.\(^8\) Consequently, most internet access in The Gambia is via dial-up at public internet cafes, which charge about US$1 per hour of access. The recent introduction of 3G wireless internet connections via mobile devices has made internet access more attainable, albeit for only a small subset of the population who can afford the unlimited 3G wireless packages that begin at about US$62 per month.

Limited access to telecommunications services in The Gambia is further compounded by a significant urban-rural divide. In general, rural areas suffer from poor or virtually nonexistent infrastructure, a lack of electricity, and frequent power cuts.\(^10\) In addition, network coverage of rural areas has not been an investment priority for most service providers,\(^11\) making rural provinces in The Gambia some of the most “disconnected regions of the world.”\(^12\) Radio remains the principal mass medium through which most Gambians stay informed.

Restrictions on Connectivity

The Gambian government’s control over the country’s telecommunications infrastructure enables it to restrict access to the internet and mobile phone services. In a November 2012 assessment, the internet research company Renesys classified the Gambia as being at “severe risk of internet dis-

---


\(^11\) Interviews by Freedom House, February 2014.

Gambia

connection” for having no more than two direct connections to the international internet, alongside repressive countries such as Ethiopia, Egypt, and Syria.\(^{13}\)

The state-owned telecom company, Gambia Telecommunications Company Limited (Gamtel), owns the fiber-optic cable that runs across the country and controls the country’s connection to the international internet via the ACE (Africa Coast to Europe) submarine cable system, allowing private telecoms to lease access to the gateway for data services.\(^{14}\) In a positive step, the government began liberalizing gateway services in May 2013 by granting international data transmission licenses to private telecom operators,\(^{15}\) though it was unclear how many new licenses had been issued as of mid-2015.\(^{16}\) The government also launched the country’s first internet exchange point (IXP) in July 2014 to boost speed, security, and affordability of internet services across the country.\(^{17}\) As of mid-2015, no issues of government control over the new IXP have been reported. Fixed-line voice communications, on the other hand, remain purely state-owned and controlled, seen mostly as part of the government’s effort to protect Gamtel’s monopoly.

A number of internet blackouts lasting several hours occurred during the coverage period, especially between August and October 2014, according to multiple sources.\(^{18}\) Service providers mostly blamed the blackouts on “technical problems and maintenance work” at the gateway, while the gateway (mainly controlled by Gamtel) blamed the disruptions on problems with the ACE cable.\(^{19}\)

In April 2015, internet service was shut down completely for one week,\(^{20}\) which providers also blamed on technical issues with the ACE cable, though some local observers believed the disruptions were a result of the government’s increasing efforts to test new ways of controlling access to the internet and critical content.\(^{21}\) The week-long internet shutdown had come only a few days after a video of a police officer beating a schoolgirl went viral on Facebook in late March,\(^{22}\) and a year after a 48-hour internet blackout in March 2014.\(^{23}\) Local observers blamed the March 2014 blackout on the government’s efforts to block VoIP applications at the time,\(^{24}\) which it succeeded in doing one week later with the popular VoIP application Viber.\(^{25}\) Viber was eventually unblocked in July 2014.

ICT Market

The Gambia’s ICT market is relatively small, with four internet service providers (ISPs)—state-owned

---

16 Interviews by Freedom House consultant, April 2015.
18 Author interviews.
19 Interviews by Freedom House consultant, April 2015.
24 Sanneh, “Gambia without internet service for 48 hours.”
Gambia

Gamtel and privately-owned QuantumNet, Netpage, and Airtip—and four mobile phone providers, all of which provide 2G/3G data service for mobile devices in country—Gamtel’s subsidiary Gamcel, and privately-owned Qcell, Africell, and Comium.

The telecommunications sector is not well regulated, and like many other sectors, businesses must contend with inefficient bureaucracies coupled with nepotistic and preferential practices conducted by government officials. Top regime officials often have working relationships with business entities and investors “across all sectors of the economy,” according to local observers. Registration for internet and mobile phone service providers is an onerous and expensive process with numerous requirements to fulfill. In addition, corruption among the authorities is rife. For example, when Qcell, one of the leading GSM companies in country, was forced to suspend its mobile money service known as QPOWER in 2013, it reportedly gifted two new cars to Gambian President Yahya Jammeh for his birthday, which led to a subsequent resumption of the QPOWER service.

Internet cafe operators must also contend with onerous, expensive, and opaque regulatory obstacles. For example, under an April 2013 directive, cybercafe owners are required to register with the regulatory agency for an operating license (in addition to a requisite business license) through an application that requires details of the ISP, the number of computers installed, and services provided. Cybercafes must renew their licenses every year and pay annual renewal fees of US$ 20 to the regulatory body or face closure. In September 2013, the regulator issued further guidelines that dictated specific requirements on the physical layout of cybercafes and the signs that must be displayed. Since 2013, more than a dozen cafes have closed down as a result of the economic obstacles imposed by the strict regulations, alongside increasing access to mobile internet.

Regulatory Bodies

The telecommunications sector is regulated under The Gambia Public Utilities Regulatory Authority Act 2001, which established the Public Utilities Regulatory Authority (PURA) in 2004 to regulate the activities of telecom service providers and other public utilities. To some consumer activists, PURA has been an ineffective regulator that seems more concerned about its image than the interests of consumers. As it stands in 2015, PURA neither has the expertise, equipment, nor enforcement power to effectively carry out its mandate. Furthermore, PURA is not independent, at least in its
Gambia

composition. The president appoints the governing board of the regulatory body on the recommendation of the Minister of Finance and Economic Affairs.37

Limits on Content

Dozens of independent online news and opposition websites remained blocked in The Gambia, amid a number of anecdotal reports of politically sensitive content “disappearing” from the internet due to intimidation from government authorities. Meanwhile, a significant digital activism campaign led to the release of an activist and blogger, who was detained without charges for his work with the survey research firm, Gallup.

Blocking and Filtering

At least 20 webpages were blocked in The Gambia during this report's coverage period,38 many of which are news and opposition websites known for their criticism of the government,39 such as Gambia Echo, Hello Gambia, Jollof News, and Gainako. One of the first websites blocked in the country beginning in 2006, Freedom Newspaper, remained blocked.40 Most of the blocked outlets are based abroad and operated by exiled activists and Gambian journalists.

YouTube, Facebook, Twitter and international blog-hosting platforms are freely available, though communications applications have been blocked in the past. The popular VoIP platform, Viber, was the most recent communications tool targeted for blocking from March to July 2014.41 The government denied involvement and hinted that service providers may have engineered the block,42 while observers blamed the government given its belief that platforms such as Viber have been enabling exiled Gambian journalists to deliver politically “objectionable” information to the public.

There is no transparency behind the blocking of internet content in The Gambia, and efforts to access blocked URLs typically time out. The government denies any involvement in the blocking of critical news websites; however, state control over the country’s dominant telecommunications provider, Gamtel, gives the authorities the ability to restrict access to internet content. Expert opinions suggest that the country targets specific internet protocol (IP) addresses and domain names at the level of the internet gateway. Meanwhile, tech-savvy Gambians use virtual private network (VPNs) and other proxies to access blocked content from within the country.43

38 Interviews by Freedom House consultant, April 2014.
40 Media Foundation for West Africa, "US-based online paper inaccessible from Gambia, deliberate blocking by government suspected."
42 The then Deputy Permanent Secretary at the Ministry of Information and Communication Infrastructure, Mr Lamin Camara was quoted saying: “The blockade of Viber has nothing to do with Public Utility Regulatory Authority (PURA), the blockage is at operators’ level. I am not pointing fingers at any operator. I know there are other services that Viber has affected and it is not good for them. We are working together to see how we can come to a better solution that would be acceptable to all parties.”
Gambia

Content Removal

The extent to which the government may require websites to take down certain content is obscured by the overwhelming number of progovernment, if not state-owned, news outlets based in the country, which often receive directives to depict the government in a positive light. Nonetheless, observers have noted an increasing trend of online content “disappearances” through anecdotal accounts from journalists and editors based in the country. A former reporter speaking anonymously revealed that he often receives orders from government officials to take down select content from certain news websites, particularly “politically sensitive” content. Some editors have reported receiving threatening phone calls for their online content, while others have experienced “visits” from officials at their offices or homes. In general, stories that risk catching the attention of security officials are highly susceptible to disappearing online, either through self-imposed post-publication censorship, or from unofficial takedown orders from government officials.

Media, Diversity, and Content Manipulation

Most critical news outlets are operated by exiled dissidents based abroad and blocked within the country. Independent online media outlets face the challenge of economic sustainability in a country where many businesses avoid advertising with critical outlets out of fear of government reprisals. As a result, the online news and information landscape does not represent a diversity of political and social viewpoints. Furthermore, a climate of fear due to pressure from the authorities in the form of arbitrary arrests, extralegal harassment, and threats has led to a severe degree of self-censorship among journalists, both online and offline. Bloggers and online journalists based in the country typically post content anonymously, while many local online activists simply avoid posting critical content or remove content after posting to evade potential repercussions.

Comments by trolls in many online forums disproportionately distort the news and information landscape, though there is no concrete evidence that the authorities employ progovernment commenters to manipulate online content. Progovernment trolling activity tends to surge during times of political or social controversy. For example, following the illegal detention of a local activist in November 2014 (see “Digital Activism”), a mass online mobilization campaign to secure the activist’s release attracted a trove of so-called “neutral” commentators who posted progovernment comments that diluted the campaign’s message. More often than not, online conversations between activists and regime apologists become abusive, resulting in quarrels, stand-offs, and sometimes the use of hate speech.

Despite the highly restrictive environment for bloggers and internet users, there are a small number of locally based independent journalists and netizens working courageously to push the boundaries of free expression and internet freedom from within The Gambia, as exemplified by two popular

44 Interviews by Freedom House consultant, April 2015.
45 Interviews by Freedom House consultant, April 2015.
47 “Since we are not all technically skilled, sometimes when we post critical information online, which in our context is incriminating, we simply delete. Sometimes the removal is accompanied by an apology or a rejoinder. This is how we survive, special circumstances present special approaches,” said a local online journalist. Interviews by Freedom House consultant, 2015.
Gambia

news blogs, Front Page International (FPI)\textsuperscript{48} and Gambia Affairs,\textsuperscript{49} which are both managed and published by journalists based in country.

Digital Activism

Digital activism is growing in The Gambia, though efforts are usually small and unsuccessful, mainly due to heavy-handed government repression against criticism and dissent. During the coverage period, one notable case of digital activism yielded a positive impact. In November 2014, the authorities released activist and blogger Sait Matty Jaw following a sizable online mobilization campaign organized by both local and international supporters using the Twitter hashtag #FreeSaitMattyJaw.\textsuperscript{50} He was reportedly arrested alongside two peers for their allegedly unauthorized work with the survey research firm Gallup.\textsuperscript{51} The online mobilization efforts also involved plans for mass public demonstrations to demand Jaw's immediate release,\textsuperscript{52} which prompted the authorities to release Jaw after holding him without charges for over a week.\textsuperscript{53}

Violations of User Rights

An opposition supporter was prosecuted in July 2014 for using Skype on his iPad to transmit coverage of an opposition rally to the Freedom Newspaper independent online outlet based abroad. Found guilty, he was ordered to pay a fine of approximately US$1,250 or spend one year in prison. A former journalist was arrested in August 2014 and accused of sending sensitive information to “enemies” of the government based abroad; he fled the country after enduring torture while in detention. Increasing incidents of extralegal intimidation and violence against several bloggers and online journalists led many to join their traditional media counterparts in exile.

Legal Environment

The 1997 constitution guarantees freedom of speech and press freedom, though fundamental freedoms are severely restricted in practice. President Jammeh is known for his utter disregard for constitutional rights, stating publicly in March 2011 that he would “not compromise or sacrifice the peace, security, stability, dignity, and the well-being of Gambians for the sake of freedom of expression.”\textsuperscript{54}

Meanwhile, a number of draconian laws further undermine freedom of expression, and in recent years, the government has successfully amended existing legislation to increase penalties for certain offenses. The criminal code, which already criminalizes defamation with a minimum prison sentence

\textsuperscript{49} Gambia Affairs, website, \url{http://gambiaaffairs.com/}.
\textsuperscript{50} Twitter, #FreeSaitMattyJaw, \url{https://twitter.com/hashtag/FreeSaitMattyJaw?src=hash}.
\textsuperscript{51} Kelly Barber, “#FreeSaitMattyJaw: African SFL Leader Detained for Over 5 Days,” Students For Liberty (blog), November 11, 2014, \url{http://bit.ly/1QaR7Mz}.
\textsuperscript{53} Weeks later, Jaw was re-arrested and put on trial but was eventually acquitted and discharged by a magistrate court, though his co-accused had pleaded guilty and paid fines. Prosecutors have however, filed an appeal against the decision.
\textsuperscript{54} Baboucarr Senghore, “President Jammeh meets with the Independent Press,” The Point, March 17, 2011, \url{http://bit.ly/1R190m}. 

326
Gambia

of one year plus heavy fines, was amended in April 2013 to penalize individuals for “giving false information to public servants” with up to five years in prison, up from six months.\(^{55}\) Observers believe the increased penalty was an effort to intimidate journalists and whistleblowers from seeking legal recourse for the physical abuse they often experience at the hands of the authorities.\(^{56}\)

Harsh legislation specifically targeting ICTs was passed in July 2013 in the form of amendments to the 2009 Information and Communication Act. Under the new amendments, online dissent is specifically criminalized with penalties of up to 15 years in prison, fines of up to GMD 3 million (about US$100,000), or both, for using the internet to criticize, impersonate, or spread false news about public officials.\(^{57}\) According to analysis by the blocked online news outlet, Gainako, the government introduced the harsh internet law in response to online activism and the growing influence of critical news outlets, stemming primarily from abroad.\(^{58}\)

Prosecutions and Detentions for Online Activities

Arrests and prosecutions of online journalists and ICT users for ICT activities are common in The Gambia. In July 2014, opposition supporter Lasana Jobarteh was prosecuted under the restrictive 2013 amendments to the communications law on charges of broadcasting a political rally in December 2013 without a license.\(^{59}\) Jobarteh was using Skype on his iPad to transmit coverage of the rally to the independent *Freedom Newspaper* online outlet based abroad, which the authorities arbitrarily determined to be a violation of the broadcast license requirements under the Information and Communications Act.\(^{60}\) He was sentenced to one year in prison or fined GMD 50,000 (about US$1,250), the latter of which was paid with support from members of his opposition party to avoid prison.\(^{61}\)

In August 2014, Abdou Jeli Keita, a former journalist for the news outlet *Foroyaa*, was arrested and accused of sending sensitive information to “enemies” of the government based abroad.\(^{62}\) At the time of his arrest, Keita was a government employee who had left journalism after previous experiences with extrajudicial detentions for his reporting. While in detention, Keita recounted how the authorities illogically presented him with old articles he had written for *Foroyaa* from his time as a journalist as evidence of his continued connection with the independent outlet. After enduring two days of torture and threats, he was released without charges and subsequently fled the country to Senegal.

In August 2015, the Managing Director of the independent radio station Taranga FM, Alagie Abdoulie Ceesay, was arrested and charged with sedition and publishing false news for allegedly circulating...
Gambia

images of the president via his mobile phone and on Facebook. He was denied bail and remains in prison while awaiting trial as of October 2015.

Citizens were also subject to harsh penalties for violating the country’s strict laws prohibiting blasphemy. In August 2015, Facebook user Alhagie Mam Seye was arrested for sharing a picture of the Prophet Mohamed on Facebook. He was subsequently charged with “uttering words with intent to wound religious feelings” and released on bail after his lawyer appealed on behalf of his mental stability. His case remained open as of October 2015.

Surveillance, Privacy, and Anonymity

Unchecked surveillance of ICTs is a grave concern in The Gambia. Section 138 of the 2009 Information and Communications Act gives sweeping powers to national security agencies and investigative authorities to monitor, intercept, and store communications in unspecified circumstances while also giving the regulator, PURA, the authority to “intrude communication for surveillance purposes,” all without judicial oversight. In addition, service providers are required to “implement the capability to allow authorized interception of communications.” The government also places restrictions on anonymous communication through SIM card and local domain name registration requirements, the latter of which is managed by the regulatory authority.

As a result, observers believe the government proactively monitors and intercepts citizens’ communications, particularly the communications of activists and independent journalists whom the government perceives as a threat to national security. Intercepted phone and email communications are often used as evidence in trials against government critics. However, the scope of the government’s technical surveillance capabilities remains unknown.

Intimidation and Violence

Gambian journalists face a high degree of violence for independent and critical reporting. In October 2014, an online journalist with the privately owned Standard newspaper, Ousman Bojang, was reported missing. Mr. Bojang, a former intelligence operative, later surfaced in neighboring Senegal and revealed that he escaped after suffering severe torture at the hands of his former colleagues at the notorious National Intelligence Agency (NIA) on allegations of sending sensitive information to the Freedom Newspaper online outlet based abroad. The former journalist, Abdou Jeli Keita, who was

70 Freedom House Interviews, February 2014.
Gambia

arrested in August 2014 (see “Prosecutions and Detentions for Online Content”) also reported being tortured by security officials while in detention.

Intimidation and threats are also common tactics used to suppress freedom of expression online. In late 2014, the government revoked the state-funded scholarship of a Gambian college student studying abroad at the University of California, Santa Barbara for posting a Facebook status in support of gay rights.73 In May 2015, Saikou Ceesay, the managing editor of the online newspaper, *Gambia Affairs*, received death threats for a Facebook post he wrote about presidential term limits.74

As a result of the unsafe environment for media workers, a growing number of bloggers and online journalists joined their traditional media counterparts in exile in 2014 and 2015,75 including two online journalists for the *Standard* news outlet, Sanna Camara and Sainey MK Marenah, who both fled the country in late 2014 following police harassment for their reporting.76

**Technical Attacks**

Opposition websites and critical online news outlets frequently experience technical attacks, which are widely believed to be perpetrated by the government. In May 2014, an independent news outlet reported leaks of a government plot to launch hacking attacks against diaspora journalists for the online news outlets, *Kairo News* and *Freedom Newspaper*.77 In November 2014, malicious malware known as “Blackhat SEO” was reportedly discovered on government websites, placing users visiting those websites at risk of infection. Local observers suspected that the malware aimed to bait and gather intelligence on online activists, especially activists based abroad.78

---

Georgia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>26</td>
<td>24</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 4.8 million  
Internet Penetration 2014: 49 percent  
Social Media/ICT Apps Blocked: No  
Political/Social Content Blocked: No  
Bloggers/ICT Users Arrested: No  
Press Freedom 2015 Status: Partly Free

Key Developments: June 2014 – May 2015

- Amendments to Georgia’s legislation introduced a “two-key” system for authorizing wiretapping, which requires the Ministry of Internal Affairs to obtain permission from the Personal Data Protection Inspector, in addition to a court order, prior to conducting surveillance. However, this provision in the final amendments does not apply to internet data, and maintains that the Ministry will have direct access to telecom servers, rather than requiring that they request the data from the telecom providers (see Surveillance, Privacy and Anonymity).

- Internet access in Georgia continues to improve, as the government moves forward with plans to ensure access to high-speed internet throughout the country by 2017 (see Availability and Ease of Access).

- The use of information and communications technologies (ICT) by activists for waging effective online campaigns has increased significantly, indicating the growing impact of internet use for disseminating information and mobilizing people for a common cause (see Digital Activism).
Georgia

Introduction

Internet access and usage continues to grow rapidly in Georgia, particularly as interest in connecting with friends through social-networking sites has increased in recent years. State bodies and several key politicians have also increased their use of the internet and modern social media tools to share information with citizens and attract attention from the potential electorate. The government continues to set up new online services, including the portal Data.gov.ge, which is intended to unite all major government data sets in the near future. However, not all government institutions express willingness to communicate effectively and directly with citizens; as a consequence, one-way interaction prevails on the websites of these agencies.

On November 30, 2014, the parliament of Georgia adopted controversial amendments related to surveillance and wiretapping. The amendments establish a “two-key system,” where one “key” to surveillance records is kept in the Ministry of Internal Affairs (MIA) and the other at the Personal Data Protection Inspector’s Office, who must verify that the surveillance action taking place is in accordance with an obtained court order. A court order is required for wiretapping or for accessing the content of communications; metadata is accessible without a warrant. There are still concerns that allowing the MIA to maintain direct access to telecom operators’ networks could compromise privacy protections.

The mandate to extend the powers of the Personal Data Protection Inspector, implemented on November 1, 2014, as well as measures to enhance national legislation related to protection of privacy, and to establish efficient guarantees for the protection of human rights and freedoms, in compliance with international standards, can be highlighted as positive developments for safeguarding ICT users’ rights. If the new agency is given sufficient power to operate and remain autonomous in its functions, there might be tangible and substantial improvements to consumers’ rights in the near future.

Additionally, new regulations were introduced for the process of nominating the leadership of the Georgian National Communication Commission (GNCC). As of October 2013, the chairperson of the commission is nominated by other commissioners of the GNCC, rather than directly by the president. Recent developments showed that this agency is still vulnerable to potential interference from the executive branch of the government.

Georgians continue to use social media tools alongside broadcast and print media to document and respond to significant political and social events. The advent of diverse interactive maps and platforms enables users to report to matters of their concern. The number of online campaigns launched by activists and civil society members has significantly increased over the past years.

Restrictions on online content in Georgia have decreased over the past few years. There are no indications of censorship or content being blocked by the Georgian authorities or internet service providers (ISPs), and there are no recent cases of activists or reporters being questioned or arrested for their online activities.¹

Obstacles to Access

The number of internet and mobile phone subscriptions in Georgia continues to grow, but high prices for services, inadequate infrastructure, and slow internet speeds remain obstacles, particularly for those in rural areas or with low incomes. The government has announced plans to address these challenges during the next few years; however, the exact strategy to overcome the digital divide has not yet been outlined.

Availability and Ease of Access

Internet access continued to grow during the reporting period. According to the International Telecommunication Union (ITU), 49 percent of the population had access to the internet in 2014, compared to 43 percent in 2013 and 20 percent in 2009. According to a countrywide survey conducted by the Caucasus Research Resource Centers (CRCC), 30 percent of the population accessed the internet on a daily basis in 2013, and the most active internet users were located in the capital. Only 5 percent of Georgians are unfamiliar with the internet altogether. There is a slight gender gap, as over 47 percent of men use the internet compared to 42 percent of women.

ISPs offer DSL broadband, fiber-optic, HSPA/EVDO, WiMAX and Wi-Fi connections. Since 2015, LTE 4G internet access has slowly become available for Georgian consumers. The average cost for an internet connection is US$20 per month, and the lowest price for a 10 Mbps DSL connection is about US$15 per month. There were approximately 603,000 fixed-line broadband internet connections in 2014, up from about 419,000 in 2012.

Mobile phone penetration is greater than that of the internet and has continued to grow from 64 percent in 2009 to 125 percent in 2014. Mobile phones significantly outnumber landlines, and reception is available throughout the country, including rural areas. However, the vast majority of households access the internet from a home computer or laptop (82 percent) rather than from personal mobile phones (12 percent). The use of mobile devices to connect to the internet may be limited by high costs (more than US$38 for unlimited internet access). However, some providers are offering new and somewhat less expensive services, including CDMA and EVDO technologies.

The GNCC introduced mobile number portability in February 2011 and fixed-line number portability in December 2011, giving users more freedom to switch between service providers and choose be-
Georgia

tween price plans.\textsuperscript{12} As of December 2014, about 442,000 subscribers had made use of this service.\textsuperscript{13} According to a new national numbering plan, as of January 2012, all phone numbers have changed to align with international standards.\textsuperscript{14}

The government of Georgia lacks a comprehensive strategy outlining a clear and long-term vision for developing internet infrastructure throughout the country. In February 2014, the government established Georgia’s Innovation and Technology Agency,\textsuperscript{15} to promote the use of innovation technologies in various fields and the commercialization of innovative technology research and development. Among other programs, it is tasked with elaborating and implementing a concept for ensuring broadband internet access to all citizens (precisely, at least 2,000 settlements) by the end of 2017.\textsuperscript{16} For these purposes, the government plans to establish a trunk cable system and take several measures, such as the liberalization of the telecommunication sector, breaking up of monopolies, completion of the transition from analogue to digital terrestrial broadcasting, and the simplification of administrative procedures.

Additionally, in order to promote the strengthening of e-governance services in Georgia, the Data Exchange Agency of the Ministry of Justice created an “e-Georgia” strategic document for the years of 2014-2018.\textsuperscript{17} Along with other goals, the “e-Georgia” strategy aims to ensure secure and effective e-services for citizens, businesses, and the non-governmental sector, based on reliable and trustworthy infrastructure. According to the report, the strategy aims to stimulate the demand and increase the use of e-services by citizens and businesses through high quality, efficient, effective, trusted and secure service delivery.

Cybercafes provide access at reasonable prices, but are located mainly in large cities, and there are too few to meet the needs of the population. They have become a popular place for online gamers, where youth spend hours playing online games. Many restaurants, cafes, bars, cinemas, and other gathering places provide Wi-Fi access, allowing customers to use the internet on their personal laptops or other devices. As part of a plan to improve infrastructure for local self-governance, in 2013 the State Services Development Agency began developing community centers where local citizens can access the entire internet and utilize resources including Skype, bank services, telecommunication services, and electronic services developed by the state (for example: property registration, e-auction, business registration, etc.).\textsuperscript{18} As of May 2015, 21 centers are operating in different regions and districts throughout the country.

Restrictions on Connectivity

The Georgian government does not place any restrictions on connectivity, and the backbone internet infrastructure is owned and operated by private companies. Despite, expanding internet access, many users complain about the quality of connections and suffer from frequent outages. For

\textsuperscript{12} Mobile price plan calculator: \url{http://online.gncc.ge/MobileCalc/MobileCalc2.aspx}. The Calculator gives users the ability to choose best plan and pricing options between mobile operators.

\textsuperscript{13} Georgian National Communication Commission, \textit{Annual Report 2014}.

\textsuperscript{14} Phone numbers now all begin with 0 and 00 prefixes.

\textsuperscript{15} Official website of Georgia’s Innovation and Technology Agency, assessed March 3, 2015 \url{http://gita.gov.ge/en/agency}.

\textsuperscript{16} Ministry of Economy and Sustainable Development of Georgia, “High Quality Internet to be Accessible to Every Region in Georgia”[in Georgian] January 15, 2015, assessed March 2, 2015, \url{http://bit.ly/1RH2mqg}.


\textsuperscript{18} Find the information about the project: State Services Development Agency, “Community Center,” [in Georgian] \url{http://sda.gov.ge/?page_id=5555}. 333
instance, according to the latest report of the GNCC, 62 written, 60 telephone and 68 oral appeals were submitted by users in 2014, out of which 28 were complaints about the poor level of telecommunication service.\textsuperscript{19}

The telecommunications infrastructure in Georgia is still weak, and users may experience disconnections from the international internet up to two or three times per month for a few minutes at a time, allowing them to access only Georgian websites, since in general, connection speeds are faster for accessing content hosted in Georgia than for international content. There are many factors influencing the connection to the international backbone, including the major underground fiber-optic cable that is often threatened by landslides, heavy rain, or construction work along the road. However, contrary to instances in recent years when access throughout the entire country was disrupted, no significant outages were reported in 2014-2015.

\section*{ICT Market}

According to the Law of Georgia on Electronic Communications, telecommunications companies must be licensed before offering services. There are currently up to 40 entities registered as ISPs in Georgia, 10 of which are large networks of governmental services or corporations that are closed to the public and serve only their own employees or branches.\textsuperscript{20} Most ISPs are privately owned, and two ISPs control more than two-thirds of the market: SilkNet, with about 49 percent of the market, and Caucasus Online with a 33 percent share. Consequently, competition on the internet market is quite low.\textsuperscript{21} For example, 15 companies provide only 1 percent of the users in the capital with internet access.\textsuperscript{22} Three ISPs—Geocell, Magnostic and Mobitel—are also mobile operators. The mobile internet market is also dominated by two main providers, Magnostic and Geocell.\textsuperscript{23}

\section*{Regulatory Bodies}

The GNCC is the main media and communications regulatory body and is also responsible for regulating online media, although there have yet to be many test cases regarding the latter. The GNCC mostly deals with mobile operators, as well as television and radio broadcasting licenses. There is no significant difference between GNCC procedures for handling traditional media and those pertinent to telecommunications and internet issues. Criticism surrounding the commission’s alleged lack of transparency and flawed licensing procedures for traditional media may reappear in the context of internet regulation. Moreover, independent and autonomous functioning of the regulatory body has always been a matter of controversy for civil society of Georgia.

In order to increase the legitimacy of GNCC, new rules for the nomination of candidates and the selection of the Head of Commission came into force on October 27, 2013. A new chairman of the agency was elected by the commissioners themselves instead of the president of Georgia in May.

---

\textsuperscript{19} Georgian National Communication Commission, Annual Report 2014.
Georgia

2014. Despite this positive development, the revelation that an advisor to the new chairman is also a representative with the Ministry of Internal Affairs has raised speculation that the central government is attempting to interfere in the work of the regulator and collect data on its activities.24

Limits on Content

In 2014-2015, there were no publicly reported incidents of censorship directly carried out by the Georgian government or ISPs. Web content is not subject to systematic manipulation by government agencies. On the contrary, online content is becoming quite diverse in the country, and internet users are increasingly using social media tools to organize and disseminate information about matters of public interest.

Blocking and Filtering

There is no evidence of online content being blocked in Georgia in 2014–2015. In 2011, the government temporarily blocked access to torrent sites and peer-to-peer file sharing services to discourage the illegal download of a Hollywood action film about the 2008 Russian-Georgian war.25 However, aside from this isolated incident, government blocking and filtering is not a major hindrance to internet freedom in Georgia.

YouTube, Facebook, and international blog-hosting services are freely available. Facebook is now the most popular website among internet users in Georgia, with bloggers and journalists increasingly using it to share or promote their content, gain readers, or start discussions on current events. Facebook is also used by civil society activists and others as a tool for discussion about ongoing political and social developments.

Users can freely visit any website around the world, upload or download any content, establish their own website, and contact other users via forums, social-networking sites, and instant messaging applications. ISPs still host websites with a great deal of pirated material,26 but visits to such sites have decreased and given way to social-networking, video-sharing, and news sites. Website filtering software is used within some state institutions and private companies, designed to improve worker productivity by blocking access to sites such as Facebook and YouTube. At the same time, both governmental bodies and private employers are increasingly using social media for recruitment and public relations purposes.

There are no laws that specifically govern the internet, require online censorship, or ban inappropriate content such as pornography or violent material. There are also no blacklists or other registers of websites that should be blocked. Nevertheless, all legal regulations, particularly copyright or criminal law, apply directly to internet activities using legal analogy, although so far this principle has not been exploited to impose significant internet content restrictions. However, there have been some concerns about the impartiality of past blocking decisions made by the GNCC. For example, the political nature of the 2011 decision by the GNCC to crack down on sites illegally hosting the film about the Georgian-Russian war, despite doing very little to combat online piracy in general, implies

---

26 For example, the website Adjaranet, http://adjaranet.com.
a lack of impartial decision-making. To date, however, such decisions regarding online content have been rare.

Content Removal

During the coverage period of this report, no reported cases of content removal directed at individuals or online media representatives were observed. Intermediary liability for defamatory content, which in other cases can lead to intermediaries preemptively removing or screening for such content, is limited by the Law on Freedom of Speech and Expression (2004), which states that no entity will be held responsible for defamatory content by unknown or anonymous individuals. To date, intermediary liability and forced removal of online content have not been significant impediments to online freedoms in Georgia.

Media, Diversity, and Content Manipulation

The online media environment in Georgia is becoming increasingly diverse, and content on a wide range of topics is available. Both voluntary and induced self-censorship among Georgian internet users is active to some extent. It is widely acknowledged that instances of self-censorship due to political pressure have decreased over the past two years. Representatives of particular professions sometimes prefer to abstain from expressing themselves freely on social networks. While some media representatives post their viewpoints without restrictions, other journalists consider refraining from openly judging politicians and decision-makers to be part of professional ethics. Additionally, civil servants in some cases may exhibit self-censorship in their online activities and comments due to pressure from higher officials.

While there is no systematic or pervasive government manipulation of online content, there have been cases where comments have been hidden or deleted from the official Facebook pages of high officials or public institutions. Additionally, there was evidence of public officials opening fake Facebook accounts and then following the official Facebook page of President Saakashvili during the 2012 election campaign. Until recently, there were still fake accounts that solely posted flattering comments of particular government officials. Specialists in Georgia argue that such forms of online manipulation indirectly impact freedom of expression online and hinder a healthy dialogue between different parties.

Inadequate revenues in the online news business, combined with a lack of technological knowledge, have hampered the expansion of traditional media outlets to the internet. The government’s inter-

---

27 Faig Alizada, “WILMAP: Georgia,” The Center for Internet and Society, Stanford University, http://stanford.io/1FIxwCU.
28 Focus group interview with more than 7 journalists and bloggers, November 25, 2013.
29 Case of an employee at LEPL of the Ministry of Environment and Natural Resources Protection of Georgia reported by the online platform – Freedom to Internet - devoted to reporting cases of violations of Internet Users’ Rights (censorship / surveillance / privacy / cases of repercussions for on-line activity / filtering and blocking of websites etc.) – See the full description of the case: Freedom to Internet, “LEPL at the Ministry of Environment and Natural Resources Protection of Georgia,” August 22, 2014, http://www.freedomtointernet.com/case/56.
30 For instance, during the reporting period, an official statement of the Ministry of Defense of Georgia, posted on its official Facebook page, was highly criticized by online activists, however almost all comments were deleted by the page administrator(s). Later this post was removed from the page.
Georgia

Interest in blogging and social media could help spur traditional outlets to establish a greater internet presence, but this would also require more private investment in online advertising. Currently, it is estimated that annual spending on online advertising does not exceed US$1 million, which is only about one percent of the total amount spent in the Georgian advertising market. At present, most online media outlets face difficulty in attracting advertisers, diversifying content, obtaining multimedia skills, and competing with traditional media representatives. Less interest toward online advertisement from the private sector stems from the relatively limited scope of the online audience.

Even though the Georgian blogosphere has grown impressively, there are currently few bloggers or activists who create content that has an impact on the political agenda, or who suggest issues for discussion among online users. Minorities and vulnerable groups in general are not limited from using the internet, and are represented online through a small number of forums and blogs. During the last three years, LGBTI activists have started to use online tools for coordination, distributing information, and protesting discrimination in the public sphere. For instance, in May 2015, activists launched an online campaign, “This street is taken - there’s no place for homophobia and transphobia here!” through disseminating posters and photos expressing solidarity with LGBTI individuals.

Additionally, online media outlets, NGOs, and some public institutions have started using interactive tools such as blogs for disseminating various types of information.

The majority of internet users (72 percent) report that they connect to the internet to check social networks. Other activities frequently carried out by Georgian internet users include searching for news (53 percent), chatting via Skype (33 percent), pursuing entertainment (25 percent), and sending or receiving email (20 percent). It is worth noting that 21 percent of people considered the internet as their main source of information.

State bodies have also become increasingly active online. For example, departments in the Ministry of Justice, the Ministry of Finance’s unit for Tax Inspection, and others have developed online platforms that allow citizens to register and receive services, apply for identification cards, or file tax documentation. Since September 2013, more than 70 e-services have been integrated in a unified governmental portal, My.gov.ge, through which citizens can make online requests for public information about the government’s budget and expenses. Other services include filling out passport applications, property registration, information about real estate, outpatient services, insurance, social assistance, state pension, and others. However, this platform has not been promoted extensively, and only a limited number of users access its services on a daily basis. Additionally, a new open data portal, Data.gov.ge, has been launched by the Georgian government, containing more than fifteen types of raw data sets in machine-readable format, released by more than ten public authorities. As of May 2015, the site contained essential public data, such as number of employees of particular government agencies, including employment broken down by gender, and procurements of respective public institutions.

34 Interviews with representatives of online media outlets November 28, 2013 and November 20, 2013.
35 Focus group interview with more than 6 journalists, bloggers and online activists November 25, 2013.
36 You can find materials of the online campaign here: Women’s Initiative Supporting Group, Online Campaign, [http://on.fb.me/1L0vpdK](http://on.fb.me/1L0vpdK).
Georgia

Several state services are entering the mobile apps market; for example, the Georgian Police have created an app where users can check important information (such as administrative penalties) or pay fines associated with tickets. Additionally, several government agencies have introduced discussion platforms where people have the opportunity to express their views regarding various policy issues. Some central government institutions use social networks for the purposes of establishing direct contact with constituencies, and attempt to respond to their questions in a comprehensive manner.

Digital Activism

Different political and civil society groups post calls for action on Facebook and use social media platforms to communicate with their supporters. Even though most forms of online activism remain online without significant offline impact, the influence of such activities is gradually increasing. For example, in December 2014, an official statement by the Ministry of Defense of Georgia (MoD) on the death of a Georgian citizen killed in Ukraine triggered rampant online criticism. The statement blamed former governmental officials from the opposition party, United National Movement (UNM), for encouraging Georgians to fight in Ukraine and called on the citizens “not to yield to provocation and not to endanger [their] own lives in exchange of various offers.” Furthermore, social networks were used extensively for mobilizing and organizing demonstrations calling for the resignation of the Defense Minister. Later, MoD officials removed the statement and apologized for the “mistake of the Ministry.”

NGO representatives of the campaign “This Affects You Too” advocating for legislative changes to surveillance laws used the internet to raise public awareness about the importance of the planned amendments. Most importantly, they initiated video competitions for any interested person, which enabled citizens to be directly involved in this process. Their main messages, demands and arguments were disseminated via several online tools. Some of their proposals were taken into account during the process of amending the surveillance legislation, but the amendments were still adopted with several negative provisions.

An interactive portal called the Civil Electronic Monitoring System was established by the Civil Development Agency (CiDA), a civil society organization in Georgia, in an attempt to build up direct consultations between local government and the local population. Four large cities—Rustavi, Gori, Kutaisi and Poti—have been incorporated in the initiative. The online platform enables citizens to report information to the respective local government officials regarding various problems in their cities including utility problems, self-governance projects, local bills, civil ideas and projects, petitions, and regulations and rules.

Another civic initiative, MyAngle, implemented by Media Activism, a nongovernmental organization in Georgia, brought together media practitioners in the South Caucasus. Activists are allowed to publish a variety of self-made stories regarding social, economic and cultural issues in different for-

mats (photo, video, audio). The main aim of the networking platform is to support multimedia journalism in the region.

Violations of User Rights

Regulation of ICT surveillance has been a prominent issue in Georgia since revelations of illegal surveillance and wiretapping emerged in 2012. Amendments to surveillance legislation were passed toward the end of 2014. These included some restrictions on wiretapping and increased judicial oversight, but also problematic provisions allowing the MIA to maintain direct access to metadata. Additionally, concerns about personal data protection remain unresolved. At the same time, there were no instances of ICT users being prosecuted or detained for their online activities, and there were no reported incidents of violence or intimidation directed at ICT users.

Legal Environment

Civil rights, including the right to access information and freedom of expression, are guaranteed by the Georgian constitution and are generally respected in practice. The Law on Freedom of Speech and Expression makes it clear that other “generally accepted rights” related to freedom of expression are also protected even if they are not specifically mentioned. Furthermore, Article 20 of the constitution and Article 8 of the Law of Georgia on Electronic Communications include privacy guarantees for users and their information, though they simultaneously allow privacy rights to be restricted by the courts or other legislation. Online activities can be prosecuted under these laws—mainly in cases of alleged defamation, which was decriminalized in 2004—or under any applicable criminal law.

Prosecutions and Detentions for Online Activities

There were no cases of charges against online users for libel or other internet activities in 2014–2015. There were also no known instances of detention or prosecution.

Surveillance, Privacy, and Anonymity

In response to revelations of illegal surveillance and wiretapping during the pre-election period in 2012, local NGO representatives, under the campaign “This Affects You Too,” started advocating for legislative amendments to limit the infringement upon private life and abuse of power by entities carrying out secret investigative actions. In August 2014, the parliament passed a package of legislative amendments that increased oversight mechanisms for government surveillance practices. According to the changes, law enforcement agencies are required to present higher standards of justification to obtain a court warrant, and justified cases are limited to those that aim to ensure national security, or prevent disorder and crime.

---

Georgia

The question of accessibility to the surveillance data was addressed in subsequent amendments. Ultimately, a “two-key system” was introduced in November 2014, whereby the Ministry of Internal Affairs sustained direct access to the lawful interception management system, enabling the agency to obtain telecommunications data in real time after securing a court order. Despite maintaining access to the telecommunications data, the MIA will not be able to start interception and monitoring of communications without the permission of the Office of the Personal Data Protection Inspector, which will in turn be equipped with the second “key” to approve the interception. Civil society members consider the adopted law restrictive and insufficient, since the newly introduced “two-key system” does not apply to data transmitted through the internet.48 Shortly after the amendments were passed, the Public Defender of Georgia filed a lawsuit in the Constitutional Court against the clause in the law on electronic communications that entitles state agencies to intercept and store telecommunications data in real time, arguing that this real-time access still violates the right to private life as stated in the constitution.49 On the other hand, the latest official surveillance data showed that over the past two years, the amount of motions on wiretapping made to courts has decreased.50 The Supreme Court of Georgia undertook the obligation to proactively publish such data annually.

On November 1, 2014, the mandate of the Personal Data Protection Inspector was extended to cover the private sector. In particular, the office is authorized to check the legality of any data processing by private organizations on their own initiation or on the grounds of a citizen’s application. If a violation is found, inspectors will be able to impose measures provided for by the law, including fines.51 The mandate also includes other significant improvements that provide more guarantees for impartiality of the inspector, expanding the office’s responsibilities, and harmonizing Georgian legislation with European standards. However, the latest report on the state of personal data protection identified major challenges and deep-rooted systematic problems including: the processing of a large amount of data by public or private organizations without proper legal grounds; the illegal disclosure of personal information to other states and/or international organization; failure to limit the use of data for direct marketing campaigns.52

There are no restrictions on the use of anonymizing or encryption tools online. However, individuals are required to register when buying a SIM card. ISPs and mobile phone companies are also obliged to deliver statistical data on user activities concerning site visits, traffic, and other topics when asked by the government. Cybercafes, on the other hand, are not obliged to comply with government monitoring, as they do not register or otherwise gather data about customers.

Intimidation and Violence

During the coverage period of this report, no cases of extralegal intimidation or physical violence directed at individuals for their online activities were reported in Georgia. Furthermore, there were no reported examples of women, LGBT individuals, or members of ethnic minority populations being harassed or threatened specifically because of their use of ICTs.

Georgia

Technical Attacks

Cyberattacks against opposition websites have not been a significant issue in Georgia, with the latest major attacks occurring in 2008 and 2009 in relation to political tensions between Georgia and Russia. By the end of 2012, the Data Exchange Agency started monitoring Georgian websites for the presence of malicious codes, hacking attacks, or other suspicious activities, publishing the information regularly on their website as well as on their official Facebook page. Additionally, the Agency produced a new service called “Safe Internet - Check My IP” capable of examining the security of the IP address of users’ computers. This service informs users connected to the internet in Georgia whether their computer is infected by any virus and provides them with detailed descriptions of detected viruses. Secure DNS services enable users to automatically block harmful content by using DNS parameters offered by Cert.gov.ge.

54 CERT, Facebook page, https://www.facebook.com/certgovge
Germany

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>17</td>
<td>18</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 80.9 million
Internet Penetration 2014: 86 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2015 Status: Free

Key Developments: June 2014 – May 2015

- Ongoing disputes between media companies and search engines over ancillary copyright enforcement have affected the freedom of information landscape online (see Media, Diversity, and Content Manipulation).

- In contrast to the European Court of Justice’s rejection of the EU Data Retention Directive in 2014, the German government proposed new data retention legislation in May 2015 (see Surveillance, Privacy, and Anonymity).

- Recent reports disclosed that the German foreign intelligence service BND helped the U.S. National Security Agency (NSA) to spy on German and European citizens, politicians and companies (see Surveillance, Privacy, and Anonymity).
Introduction

The state of internet freedom in Germany is frequently and openly discussed by the media and civil society, mainly due to the prominence of internet regulation issues in widely read online news publications. There is now a general consensus that internet freedoms are essential for an open and democratic society, and politicians, both from the governing parties and the opposition, usually act accordingly.

At the same time, some important issues remain unresolved, or have even come under renewed pressure during the reporting period. For one, both the ancillary copyright for press publishers and the European Court of Justice’s ruling on the “right to be forgotten” have had an impact on the content displayed by search engines, potentially infringing on the freedom of information. The current law on the liability of providers of open access to the internet, as interpreted by a court case from 2010, remains a serious obstacle for cafes and other businesses wanting to establish free wireless networks for customers, and recent proposals by the governing coalition for new legislation fail to effectively change the legal situation for non-commercial providers. Furthermore, despite the European Parliament’s endorsement of net neutrality, there are increasing signs that the government and the ruling coalition in the German parliament are starting to back away from upholding the principle.

In the wake of the European Court of Justice’s dismissal of the EU Data Retention Directive in the spring of 2014, law enforcement representatives have found support from the governing coalition in their call for new national legislation to enact data retention in Germany. Despite growing opposition from civil society that has become more aware of surveillance issues due to whistleblower Edward Snowden’s revelations concerning the activity of the NSA and German intelligence services, the government now seems determined to introduce data retention in the near future. The NSA scandal itself has still not been properly resolved or assessed despite the ongoing parliamentary inquiry process. Even as the government is rightly being criticized for a lack of cooperation with the inquiry commission, new disclosures in April 2015 about the role of the German foreign intelligence service BND have added to the magnitude of the affair.1

Obstacles to Access

Internet access in Germany continues to grow, and there are few inhibiting obstacles to access. However, in terms of broadband development, the country still lags behind other European states, in particular outside of urban centers. In the mobile market, the merger of Telefónica and E-Plus in July 2014 has led to less competition.

Availability and Ease of Access

Germany’s network infrastructure for information and communication technologies is well-developed, with 79 percent of the population in Germany having private internet access.2 Together with the number of mobile-only internet users, this has resulted in an overall internet penetration rate of

---

Germany

89 percent, according to Eurostat findings, which is 8 percentage points above the European Union (EU) average. Similarly, data compiled by the International Telecommunications Union place the internet penetration rate at 86 percent by the end of 2014. However, growth in internet penetration is slowing, with an increase of only 0.3 percentage points in the past year. The portion of individuals who still plan on obtaining private access is 2.9 percent.

The most widely used mode of internet access is still DSL, with 23.3 million connections in 2014. However, cable internet connections are becoming more widespread, with 6.3 million connections in 2014, compared to only 5.5 million in 2013. Connections with speeds of more than 50 Mbps are available for about 66 percent of households. In 2015, the development of comprehensive broadband supply was still considered to be proceeding too slowly, according to experts at a conference in Berlin in April 2015, especially in non-urban areas. The state of Bavaria, however, has announced a push for increased efforts by providing vast public funding. On the federal level, Minister for Traffic and Digital Infrastructure Alexander Dobrindt announced a joint roadmap with industry to provide every household with internet access speeds of at least 50 Mbps by 2018. He reaffirmed the federal government’s commitment in March 2015, announcing that the federal government and telecom companies would invest a combined amount of 10 billion euros in 2015.

Mobile phone penetration in Germany is nearly universal, with a penetration rate of 139 percent. In 2014, internet access via mobile devices further increased: 52.6 million people regularly accessed the internet via UMTS or LTE, compared to only 36.9 million in the year before. The total data volume increased from 267 million GB in 2013 to 393 million GB in 2014. According to the Federal Ministry of Economics and Technology, Germany is ranked ninth internationally in terms of mobile internet access. In February 2015, 45.6 million people in Germany used a smartphone. By the end of 2014, LTE connections with at least 2 Mbps were available to 92.1 percent of all German households, while connections with at least 6 Mbps were available to 74.7 percent. A year before, these numbers had been only 70 and 44 percent, respectively.

10 "Dobrindt kündigt Milliarden-Invesition in Breitbandbau an," [Dobrindt announces investment of billions of Euros in broadband development],
11 Bundesnetzagentur, Jahresbericht 2014, 79.
12 Bundesnetzagentur, Jahresbericht 2014.
13 Bundesnetzagentur, Jahresbericht 2014.
16 Bundesnetzagentur, Jahresbericht 2014, 80.
17 TÜV Rheinland Consulting, mid-2013, p. 4. With the allocation of licenses for the next generation mobile standard LTE, the Bundesnetzagentur has obliged the network providers to build the new infrastructure in rural areas first before installing it cities.
Germany

There is still a gender gap when it comes to accessing the internet in Germany. While 81.8 percent of men used the internet in 2014, only 71.9 percent of women did. The difference stagnated at 9.9 percent compared to 9.6 in 2013. Internet penetration is particularly high in the age group between 14 and 39 (over 96 percent) but, in comparison, relatively low in the age group 70 and above (about 30 percent). Despite considerable and stable growth rates in the preceding years, the rate of internet penetration in this latter group has stagnated in the past year.

Differences in internet usage depending on formal education level have not significantly changed over the past few years: the discrepancy between people with low and high levels of formal education is still noteworthy. This phenomenon is confirmed by a comparison of net household incomes. Households with less than EUR 1,000 (US$1,283) net income per month have a 54.1 percent penetration rate, whereas those with more than EUR 3,000 (US$3,848) net income have a penetration rate of 93.7 percent. Furthermore, slight differences in internet usage exist between Germany’s western region (79 percent) and the eastern region that once constituted the communist German Democratic Republic (71 percent); in the past year, this difference has even slightly increased. The gap between the urban states Hamburg, Berlin, and Bremen, and the rural states with the smallest internet penetration rate such as Saxony-Anhalt or Brandenburg, has again slightly decreased but is still between 10 to 14 percent. Although the governing coalition on the federal level has acknowledged these digital divides as problematic, the discrepancies in access persist.

Prices for internet access have remained relatively stable, while telecommunication services have become slightly less expensive, decreasing by about 1.6 percent. The available figures indicate that prices for flat rate broadband internet still range from EUR 16 to EUR 30 (US$21 to US$38) which is regarded as affordable compared to the average income per household of EUR 3,989. Nevertheless, as the stark differences in internet usage compared to income indicate, the price level constitutes a barrier for people with low incomes and the unemployed. Although the Federal Court of Justice ruled that access to the internet is fundamental for everyday life, costs for internet access are not adequately reflected in basic social benefits.

Restrictions on Connectivity

The German government does not impose restrictions on ICT connectivity. The telecommunications infrastructure in Germany was privatized in the 1990s and is largely decentralized today. There are

Germany

more than one hundred backbone providers in the country. The former public enterprise Deutsche Telekom was privatized in 1995, and remains the only company that acts as both a backbone provider and an ISP. However, the German state owns less than a third of its shares, which crucially limits its control over Deutsche Telekom. There are a number of connections in and out of Germany, the most important being the DE-CIX, which is located in Frankfurt. It is privately operated by eco, the Association of the German Internet Industry.

ICT Market

The telecommunications sector was privatized in the 1990s with the aim of fostering competition. The incumbent Deutsche Telekom’s share of the broadband market is currently 42.1 percent, which marks a further decline as competition continues to increase. Other ISPs with significant market share include Vodafone/Kabel Deutschland combined with 18.2 percent, 1&1 with 14.3 percent, cable companies Unitymedia Kabel BW with 9.9 percent, and O2-Telefónica with 7.3 percent. Despite the merger of Vodafone and Kabel Deutschland, the leading position of the Deutsche Telekom is still virtually unchallenged.

There are now three general carriers for mobile internet access: T-Mobile, Vodafone, and E-Plus/O2-Telefónica. Due to the merger of E-Plus and O2 in July 2014, the new company has gained market leadership with 44.7 million customers. Former leader T-Mobile follows with 39.1 million. Vodafone had 32.3 million customers in 2014. Before the merger, the German market was considered one of the most competitive in the European Union. With main competition reduced to three providers, there is some fear that this may change at the expense of a favorable pricing development. Nevertheless, the EU Commission approved the deal after a formal investigation.

Regulatory Bodies

Internet access, both broadband and mobile, is regulated by the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway (Bundesnetzagentur or BNetzA), which has operated under the supervision of the Federal Ministry of Transport since early 2014. The president and vice president of the agency are appointed for five-year terms by the German federal government, following recommendations from an advisory council consisting of 16 members from the German Bundestag and 16 representatives from the Bundesrat. The German Monopolies Commission and

29 In January 2015, Vodafone announced that it would soon drop the name of Kabel Deutschland, the company it had acquired in 2013; Caspar Busse, “Kabel Deutschland – ein Name verschwindet,” [Kabel Deutschland – a name disappears] Sueddeutsche, January 28, 2015, http://bit.ly/18Cmy2s.
Germany

the European Commission (EC) have both criticized this highly political setting and the concentration of important regulatory decisions in the presidential chamber of the Federal Network Agency. Similarly, the European Court of Justice (ECJ) and the EC noted that the regulation of data protection and privacy by agencies under state supervision does not comply with the EU Data Protection Directive 95/46/EC.

In addition to such institutional concerns, regulatory decisions by the BNetzA have been criticized for providing a competitive advantage to Deutsche Telekom, the former state-owned monopoly. The most recent examples are the agency’s decisions on April 10, 2013 to allow a slight increase in the price that Telekom charges competitors for the “last mile,” the final leg of telecommunications infrastructure that reaches customers, and to support controversial vectoring technology, which in turn manifests its dominant position regarding the last mile. Vectoring can boost the bandwidth of DSL connections on existing copper lines but requires one operator to manage the whole bundle, in effect limiting the unbundling of the local loop and thus privileging, under specific circumstances, the market leader. Despite the widespread concerns about a “re-monopolization” of the fixed-line network, the BNetzA announced its final decision on August 29, 2013, after making some adjustments in favor of Telekom competitors and subsequently obtaining the approval of the EU Commission.

Limits on Content

Access to online content in Germany is relatively free, and most often restricted content involves copyright issues or disputes concerning the remuneration of authors. Some further limitations that potentially affect freedom of expression and freedom of information stem from the ongoing enforcement of the ancillary copyright for press publishers and the European Court of Justice’s decision on the right to be forgotten in May 2014.

Blocking and Filtering

Government-imposed blocking of websites or internet content rarely takes place in Germany. In
2014-2015, there were no publicly known incidents of censorship directly carried out by state actors. Since there is also no significant filtering of text messages or email communication, the overall scale and sophistication of censorship has remained stable and on an insignificant level. YouTube, Facebook, Twitter and international blog-hosting services are freely available.

Content blocking or filtering practices enforced by corporate actors have been discussed for some time. The ongoing dispute between YouTube and GEMA (German Society for Musical Performance and Mechanical Reproduction)\(^43\) indicates that private entities substantially shape the availability of online content.\(^44\) Since 2009, Google and GEMA have been unable to reach an agreement on the amount Google should pay for a license for copyright-protected music videos disseminated on YouTube. GEMA considers it a copyright violation when YouTube uses "the rights administered by GEMA without paying any compensation to the copyright owners."\(^45\) As a result of this disagreement, which as of May 2015 remains unresolved, YouTube blocks videos for users within Germany if the video might contain copyrighted music, instead showing an error message saying that the video is not available in Germany because GEMA might not have granted the publishing rights.\(^46\) Google has raised concerns about the resulting undesired harms for freedom of expression.\(^47\) In February 2014, the Munich District Court decided in an injunction suit filed by GEMA that the phrasing of YouTube’s error message violated the collecting society’s rights.\(^48\) Although YouTube subsequently altered the content of the displayed message on blocked videos,\(^49\) the Higher Regional Court in Munich confirmed the lower court’s judgment, arguing that the displayed message kept misleading viewers by implying GEMA’s responsibility for the blocking of content.\(^50\)

German ISPs employ deep packet inspection (DPI) for the purposes of traffic management, as well as to throttle peer-to-peer traffic. Users are especially affected by P2P-related restrictions in the mobile market.\(^51\) Although Vodafone, for example, announced that for the time being the practice shall remain limited to mobile internet access, there is no ultimate confirmation that it will not be extended in the future.\(^52\)

---

43 Collecting societies are private organizations at the national level in Germany authorized by the Copyright Administration Act (Urheberrechtswahrnehmungsgesetz). Although they act under the supervision of the German Patent and Trademark Office (DPMA), they belong to the private sector. With the foundation of the collecting society C3S, provided the DPMA grants permission, GEMAs national monopoly could soon come to an end, see Jens Uthoff, "Neue Wege im Paragraphendschungel," [New paths through the regulation jungle] Taz, April 9, 2014, http://www.taz.de/1136441/.

44 Compared to 0.9 per cent in the United States and ca. 1 per cent in Austria and Switzerland. Cf. Pascal Pauknet, “Diese Kultur ist in Deutschland leider nicht verfügbar,” [This culture is not available in Germany] Sueddeutsche Zeitung, January 28, 2013, http://sz.de/11584813.


46 GEMA demands 0.375 cents per retrieval.

47 In particular Google argues that because the GEMA doesn’t provide a list on the complete repertoire they licensed, most music videos have been blocked in order to avoid financial risks. Cf. http://bit.ly/1l3QK7.


The protection of minors constitutes an important legal framework for the regulation of online content. Youth protection on the internet is principally addressed by states through the Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting (JMStV), which bans content similar to that outlawed by the criminal code, such as the glorification of violence and sedition. A controversial provision of the JMStV reflecting the regulation of broadcasting media mandates that adult-only content on the internet, including adult pornography, must be made available in a way that verifies the age of the user. The JMStV enables the blocking of content if other actions against offenders fail and if such blocking is expected to be effective. The Federal Criminal Police Office (Bundeskriminalamt) has initiated the deletion of thousands of sites related to child pornography. In 2013, it reported a slight decline in discovered sites.

Content Removal

Most of the content removal issues in Germany relate to the removal of results from search engine functions, rather than deletion of content from the internet entirely. The autocomplete function of Google’s search engine has repeatedly been subject to scrutiny. In May 2013, the Federal Court of Justice ruled that Google could be held liable, at least under some circumstances, for the infringement of personal rights through its autocomplete function. In its subsequent decision concerning the same case, the Higher Regional Court in Cologne decided that Google’s liability amounted to the obligation to delete the respective automated search query combination and to refrain from repeating the tort, but not to pay further compensation.

Since the European Court of Justice decision on the right to be forgotten in May 2014, Google and other search engines have been under the obligation to remove certain search queries from their index in the case that they infringe on the right to privacy of a person, and that person files a respective application with the search engine. As of March 31, 2015, Google had assessed nearly 40,000 applications, and decided to remove the link in roughly half of the cases. In order to reduce repercussions in relation to the freedom of expression and information, a potential downside of the judgment as maintained by numerous experts, Google set up an advisory group assigned with the

---

55 Cf. the respective § 5, Abs. 3 JMStV.
task to develop formal and substantial criteria in order to adequately balance between the affected civil rights.\(^\text{63}\)

There is no censorship prior to the publication of internet content. On the other hand, figures released by ICT corporations indicate that post-publication content removal requests are issued with regard to defamation or illegal content. According to Google's latest transparency report regarding requests to remove content, covering the period from January to June 2014, the company received 151 requests from the German courts and other public authorities.\(^\text{64}\) Defamation remains by far the most common reason for court orders to remove content.\(^\text{65}\) Upon request from authorities, between July and December 2014, Facebook restricted access to 60 pieces of content that advocated right-wing extremism and Holocaust denial, which are illegal under the German criminal code.\(^\text{66}\)

The liability of platform operators for illegal content is regulated by the Telemedia Act. The law distinguishes between full liability for owned content and limited “breach of duty of care” (Störrerhaftung) for access providers and host providers of third party content.\(^\text{67}\) Although access and host providers\(^\text{68}\) are not generally responsible for the content they transmit or temporarily auto store, there is a certain tension between the underlying principles of liability privilege and that of secondary liability.\(^\text{69}\) Principally, ISPs are not required to proactively control or review the information of third parties on their servers; they become legally responsible as soon as they gain knowledge of violations or violate reasonable audit requirements.\(^\text{70}\)

In 2012, court rulings limited the liability privilege of intermediaries by further specifying requirements, responsibilities, and obligations. Additional blocking and filtering obligations of host providers have been put in more concrete terms by the Federal Court of Justice (Bundesgerichtshof, BGH) in the “Alone in the Dark” case.\(^\text{71}\) In this specific instance, the game publisher Atari sued the file hosting service Rapidshare for copyright violations concerning a video game. Although the judges did not hold Rapidshare liable for a direct infringement, they saw a violation of the service’s monitoring obligations under the breach of duty of care as a result of Rapidshare’s failure to proactively control its service for copyrighted material after it was notified of one infringing copy.\(^\text{72}\)

In a subsequent decision concerning Rapidshare in August 2013, the BGH substantiated and further extended host providers’ duties. According to the judgment, if the business model of a service aims to facilitate copyright infringements, the company is considered less worthy of protection with regard to liability privilege.\(^\text{73}\) As a consequence, host providers are required to monitor their own serv-

\(^{63}\) Google Advisory Council, How should one person's right to be forgotten be balanced with the public's right to information, February 6, 2015, http://bit.ly/1LSL0Pd.


\(^{67}\) In particular: Part 3, §§ 7-10 TMG: liability for own content (§ 7, Abs. 1 TMG); limited liability for access providers (§§ 8, 9 TMG) and host providers (§ 10 TMG).

\(^{68}\) The BGH in particular has developed the principles of limited liability of host providers: BGH [Federal Court of Justice], judgment of October 25, 2011, Az. VI ZR 93/10.

\(^{69}\) Liability privilege means that information intermediaries on the internet such as ISPs are not responsible for the content their customers transmit. Secondary or indirect liability applies when intermediaries contribute to or facilitate wrongdoings of their customers.


ers and search for copyright-protected content as soon as it has been notified of a possible violation.74 As agreed on in the coalition agreement in 2013, the Federal Ministry of Economy introduced a draft bill in March 2015 in order to legislate a revision of the law on the breach of a duty of care. It explicitly provided for a preclusion of liability privilege for providers with such business models.75

ISPs are obliged to disclose customer information for prosecutions of copyright infringement, even though the person may not have infringed copyrights for commercial purposes.76 A special requirement to review the content on any violations of rights was also ruled in a case where a blogger integrated a YouTube video onto his website.77 However, in October 2014, the European Court of Justice ruled that embedding content from other sources by means of framing is, as such, not a copyright infringement.78

An important exception to the liability privilege concerns wireless networks.79 Because of a highly disputed Federal High Court ruling in 2010 against the existing liability privilege, as it applied to wireless networks, legislative initiatives from states and political parties now seek to modify the secondary or indirect liability of local Wi-Fi operators. The governing coalition agreed to press ahead with new legislation that aims to create legal certainty for operators in order to facilitate the expansion of publicly accessible Wi-Fi networks. However, the bill introduced in March 2015 that aimed to revise the current rules on liability was criticized for only privileging commercial providers of wireless networks, not those who want to share their network access for non-commercial purposes.80 Moreover, the proposal obliges providers of freely accessible hotspots to undertake “appropriate measures” to identify users, which is problematic in relation to both practicability and the right to anonymity.81 An initiative by the parliamentary factions of the Greens and Die Linke parties to provide for a more lenient regulation concerning providers of open internet access was rejected by the governing coalition in November 2014.82 In addition to these legislative proposals, in September 2014 a Munich court asked the European Court of Justice for a preliminary ruling on the question of the applicability of the liability privilege for a provider of an openly accessible Wi-Fi network.83

79 In 2010, the German Federal High Court sentenced the private owner of a wireless router on the grounds that his or her open network allowed illegal activities. cf. Christopher Burgess, “Three Good Reasons to Lock Down Your Wireless Network,” The Blog, The Huffington Post, June 8, 2010, http://huff.to/1LYHK3k.
Germany

Media, Diversity, and Content Manipulation

Germany is home to a vibrant internet community and blogosphere; however, there are some issues with regard to the enforcement of ancillary copyright regulations that may have the effect of distorting search results for news outlets attempting to monetize their content.

While the degree to which political actors can successfully pressure online news outlets to exclude certain information from their reporting is still insignificant, there have been some attempts to delete critical information on the internet. In January 2014, the Federal Ministry of the Interior accused the website FragdenStaat.de of copyright infringement after the website had published an internal document concerning legal analysis of an election threshold for the elections to the European Parliament. The decision was criticized as an attempt to abuse copyright laws in order to suppress freedom of information. In reaction to the incident, the commissioners for the protection of the freedom of information on both the federal and state level released a joint statement rejecting the Federal Ministry of the Interior’s claims. The commissioners demanded the government clarify that copyright law may not be employed to withhold administrative information.

To date, self-censorship online has not been a significant or well-documented issue in Germany. Still, there are more or less unspoken rules reflected in the publishing principles of the German press. The penal code and the JMStV prohibit content in a well-defined manner (such as child pornography, racial hatred, and the glorification of violence). Additionally, the criminal investigation into the online media outlet Netzpolitik in July 2015, with regard to their reports on the activities of the German intelligence agencies, was criticized for its potential chilling effect on investigative reporting, even though the case was subsequently dropped.

The principle of net neutrality was legally codified with the latest amendment of the telecommunications act (Telekommunikationsgesetz, TKG), § 41a TKG, enacted in May 2012. While the European Parliament’s April 2014 vote in favor of net neutrality has widely been considered a positive step, the details of the new regulation are considered deficient and incomplete. At the same time, the principle has come under heightened pressure in Germany over the past year. The ruling coalition has started to endorse classified net traffic in order to privilege certain services and providers. In October 2014, it was revealed that the government may refrain from promoting net neutrality in order to create incentives for private companies to speed up the development of broadband internet in Germany. According to suggestions published by the Federal Ministry of Transportation, certain internet services may acquire paid priority treatment by the networks in order to refinance infrastructure.

measures in this sector.\textsuperscript{90} At the same time, EU Commissioner for the Digital Economy and Society Günther Oettinger has repeatedly argued in favor of an abandonment or modification of the principle.\textsuperscript{91} A report published in March 2015 disclosed findings that suggest that net neutrality is already frequently violated in Germany. For instance, most mobile internet providers contractually prohibit certain services such as tethering or Voice over Internet Protocol (VoIP) in order to maximize profit.\textsuperscript{92}

Local and international media outlets and news sources are generally accessible and represent a diverse range of opinions. However, the enactment of the ancillary copyright for press publishers (Leistungsschutzrecht für Presseverleger), which came into effect on August 1, 2013, allows publishers to monetize even the small snippets of information that search engine operators display as part of the results of a query.\textsuperscript{93} This raised concerns regarding the constitutionally protected rights to freedom of expression and freedom of information.\textsuperscript{94} In 2014, in reaction to the law’s enactment, search engines started to exclude search results leading to the websites of publishers who had assigned the collecting society VG Media to collect fees stemming from the ancillary copyright.\textsuperscript{95} When Google declared that in the future it would endeavor to show only such results and snippets that fall outside of the scope of the law, twelve German publishers and the VG Media initiated antitrust proceedings against the search engine, which were rejected by the Federal Cartel Office.\textsuperscript{96} Subsequently, major publisher Axel Springer reported that due to Google’s practice, traffic to its news websites had dropped by 40 percent. In reaction, several publishers including Springer granted Google a license to show snippets free of charge.\textsuperscript{97} This decision was criticized for unduly privileging the market leader while disadvantaging smaller search engines, thus further reinforcing Google’s leading position.\textsuperscript{98} In part due to this practice, the law remains controversial. However, while the parliamentary opposition seeks to revoke the law,\textsuperscript{99} the governing coalition refuses to consider succumbing to the critics.

Digital Activism

In the past year, the internet has provided the infrastructure for several advocacy campaigns concerning political and social issues in Germany. As the government’s reluctance to uphold net neutrality became apparent, internet users were encouraged to take part in an online day of action on

Germany

September 10, 2014. Aside from that, the long-term pan-European campaign for net neutrality continued, gaining renewed urgency after the aforementioned recent political developments. Likewise, two separate campaigns were launched in reaction to distinct legislative plans concerning data retention on both the national and European level. Domestically, the renewed proposals to introduce comprehensive data retention sparked vocal opposition among civil rights groups, which urged citizens to partake in online protests in order to express their objection. An even more widespread online mobilization was observed in relation to EU plans to enact obligatory data retention of the data of airline passengers. Under the hashtag #NoPNR, several websites called for a pan-European day of action on April 11, 2015.

Violations of User Rights

During the reporting period, the repercussions of whistleblower Edward Snowden’s revelations concerning the vast surveillance practices by the NSA and GCHQ continued to dominate the political agenda. While a parliamentary inquiry commission attempts to investigate the degree of spying on German citizens and politicians, the federal government has been criticized for failing to sufficiently provide the necessary information to the commission. At the same time, new disclosures have further implicated the German intelligence service BND, culminating in reports that the service was involved in industrial espionage at the expense of German and European companies.

Legal Environment

The German Basic Law guarantees freedom of expression and freedom of the media (Article 5) as well as the privacy of letters, posts, and telecommunications (Article 10). These articles generally safeguard offline as well as online communication. In addition, a groundbreaking 2008 ruling by the Federal Constitutional Court established a new fundamental right warranting the “confidentiality and integrity of information technology systems” grounded in the general right of personality guaranteed by Article 2 of the Basic Law.

In July 2014, the federal government proposed legislation to transform the Office of the Federal Commissioner for Data Protection and Freedom of Information from a subdivision of the Federal Ministry of the Interior to an independent supreme federal authority. The act, which passed the Federal Assembly on February 6, 2015, is expected to significantly strengthen the Commissioner’s

101 “Save the Internet” campaign page, https://savetheinternet.eu/.
powers in relation to data protection in Germany.  

Prosecutions and Detentions for Online Activities

Online journalists are largely granted the same rights and protections as journalists in the print or broadcast media. Although the functional boundary between journalists and bloggers is starting to blur, the German Federation of Journalists maintains professional boundaries by issuing press cards only to full-time journalists. Similarly, the German Code of Criminal Procedure grants the right to refuse testimony solely to individuals who have “professionally” participated in the production or dissemination of journalistic materials.

In the fall of 2014, during the proceedings of the parliamentary inquiry commission that was installed in the aftermath of the NSA revelations, the online journalist Andre Meister from the news website Netzpolitik.org, who blogged live from the commission, was reportedly monitored by the parliamentary police. Upon inquiry, the acting officer conceded that he was especially assigned to keep an eye on the journalist. Although the conduct was officially dismissed as a mere misunderstanding, it was met with harsh criticism, and Netzpolitik.org announced it was taking legal action against the alleged surveillance of their journalistic activity. According to the journalist, parliament officials have since responded that there is no information about him stored by the Bundestag. Moreover, as previously mentioned, editor-in-chief of Netzpolitik.org Markus Beckedahl and Andre Meister were subject to a criminal investigation for charges of treason following their reporting on the activities of the Federal Office for the Protection of the Constitution in July 2015.

The German Criminal Code (StGB) includes a paragraph on “incitement to hatred” (§ 130 StGB), which penalizes calls for violence against minority groups and assaults on human dignity. The German people mostly regard this provision as legitimate, particularly because it is generally applied in the context of holocaust denials.

Surveillance, Privacy, and Anonymity

Debates over the activities of the NSA and the British government's intelligence organization GCHQ—and the German intelligence service's involvement in such mass surveillance—continued throughout the past year. While there are few restrictions on anonymous communication and the right to anonymity is generally upheld, the surveillance revelations remain a concern with regard to protecting the rights to privacy and freedom of expression.

112 Information provided by Andre Meister.
114 Cf. fn. 54.
The ramifications of the leaked classified documents by former NSA contractor Edward Snowden regarding the activities of UK and U.S. intelligence services lingered throughout the reporting period, while new revelations surfaced. After it had already become known in 2013 that the German Federal Intelligence Service (Bundesnachrichtendienst, BND) had monitored German internet traffic on behalf of the NSA, further information reported in July 2014 disclosed that the BND had permanent access to all data traffic routed through the central node of the internet exchange point DE-CIX in Frankfurt since at least 2009, with the help of a major German internet provider. The practice was allegedly carried out with at least tacit approval of both the Office of the Federal Chancellor and the Federal Ministry of the Interior, and was deemed unconstitutional by lawyers testifying in the parliamentary commission of inquiry.

In October 2014, it was reported that the data transmitted to the NSA included that of German citizens, although the BND denied having done so deliberately. The conduct came under scrutiny at the commission of inquiry, which had been installed by the Federal Parliament in March 2014. During the hearing in March 2015, DE-CIX manager Klaus Landefeld strongly criticized the German authorities for not providing clear and transparent rules on the legal requirements for surveillance measures. Shortly thereafter, the central node operator announced a lawsuit against the BND. During the course of the inquiry commission’s proceedings, the federal government was repeatedly criticized for insufficiently cooperating with the appointed representatives, for instance refusing to transmit essential files and records. Minister of the Chancellery Peter Altmaier was even accused of threatening commission members with criminal charges after details of certain files had been published by the press.

In April 2015, German weekly Der Spiegel reported on a further dimension of the espionage scandal, disclosing that the BND had spied on German and European politicians, citizens, and companies for the NSA. In particular, the aspect of industrial espionage was widely regarded as a hitherto unthinkable breach of confidence.

---


Germany

had been informed as early as 2008 but ignored the respective reports. 129

Although the Federal Minister of the Interior and some other members of the conservative parties have repeatedly expressed their disapproval of anonymity on the internet, 130 the principle is by and large upheld as a basic right. The basic right was further strengthened by a decision by the Federal Court of Justice, which confirmed that an online review portal is under no obligation to disclose the data of an anonymous user. In the preceding judgment, the Higher Regional Court in Stuttgart had ruled to the contrary. 131 Website owners or bloggers are not required to register with the government. However, most websites and blogs need to have an imprint naming the person in charge and contact address. The anonymous use of email services, online platforms, and wireless internet access points are legal.

The right of anonymity notwithstanding, the telecommunication act of 2004 stipulates that the purchase of SIM cards requires registration, including the purchaser’s full name, address, international mobile subscriber identity (IMSI), and international mobile station equipment identity (IMEI) numbers if applicable. 132 In this way, the growing penetration of mobile internet threatens to further erode the possibility of anonymous communication.

The use of proxy servers is common in Germany, but more for the purpose of circumventing copyright restrictions than to avoid censorship. There are no figures available for the extent of their use.

Excessive interceptions by secret services formed the basis of a 2008 Federal Constitutional Court ruling, which established the new fundamental right warranting the “confidentiality and integrity of information technology systems.” The court held that preventive covert online searches are only permitted “if factual indications exist of a concrete danger” that threatens “the life, limb, and freedom of the individual” or “the basis or continued existence of the state or the basis of human existence.” 133 Based on this ruling, the Federal Parliament passed an act in 2009 authorizing the Federal Bureau of Criminal Investigation (BKA) to conduct covert online searches to prevent terrorist attacks on the basis of a warrant. 134 In addition to online searches, the act authorizes the BKA to employ methods of covert data collection, including dragnet investigations, surveillance of private residences, and the installation of a program on a suspect’s computer that intercepts communications at their source. In April of 2015, it was revealed in an audit report conducted by the Federal Commissioner for Data Protection and Freedom of Information that the BKA had gravely violated data protection law by storing the personal data of numerous left-wing political activists without sufficient legal grounds.

Several persons had been included in the database after taking part in constitutionally protected ac-

---

132 Telecommunications Act (TKG), § 111.
The amended telecommunication act of 2013 reregulates the “stored data inquiry” requirements (Bestandsdatenauskunft). Under the new provision, approximately 250 registered public agencies, among them the police and customs authorities, are authorized to request from ISPs both contractual user data and sensitive data. While the 2004 law restricted the disclosure of sensitive user data to criminal offenses, the amended act extends it to cases of misdemeanors or administrative offenses. Additionally, whereas the disclosure of sensitive data and dynamic IP addresses normally requires an order by the competent court, contractual user data (such as the user’s name, address, telephone number, and date of birth) can be obtained through automated processes. The requirement of judicial review has been subject to two empirical studies, both of which found that in the majority of cases a review by a judge does not take place. Data protection experts criticize the lower threshold for intrusions of citizens’ privacy as disproportionate. Two members of the Pirate Party and a lawyer who had already filed the complaint against the data retention law in 2007 have filed a new constitutional complaint against the telecommunication act. In the aftermath of the enactment on the federal level, several German states established their own laws, with one state’s legislation even entirely omitting the requirement of preceding judicial review. As of mid-2015, the Federal Court of Justice has not yet issued a decision on the matter.

Telecommunications interception by state authorities for reasons of criminal prosecution is regulated by the code of criminal procedure (StPO) and is understood as a serious interference with basic rights. It may only be employed for the prosecution of serious crimes for which specific evidence exists and when other, less-intrusive investigative methods are likely to fail. According to recent statistics published by the Federal Office of Justice, there were a total of 22,917 orders for telecommunications interceptions in 2013, compared to 23,687 in 2012, of which 5,033 concerned internet communications, compared to only 4,488 in the year before. There were also a total of 20,923 orders requesting internet traffic data in 2013, compared to 18,026 in 2012. Surveillance measures conducted by the secret services under the Act for Limiting the Secrecy of Letters, the Post, and Telecommunications exceed these figures. For 2013, the competent Parliamentary Control Panel reported that a total of 15,401 telecommunications – most of them email – were scanned, of which only...

---


137 Two independent studies from the Universität of Bielefeld (2003: Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung” [Who controls telecommunication surveillance? An empirical investigation on judicial overview of telecommunication surveillance], edited by Otto Backes and Christoph Gussy, 2003) and Max-Planck-Institut Institute for Foreign and International Criminal Law: Hans-Jörg Albrecht, Claudia Dorsch, and Christiane Krüpe, “Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen,” [Legal reality and efficiency of wiretapping, surveillance and other covert investigation measures], http://www.mpig.de/688492/pdf.pdf, evaluated the implementation of judicial oversight of telecommunication surveillance. Both studies found that neither the mandatory judicial oversight nor the duty of notification of affected citizens are carried out. According to the study by the Max Planck Institute, only 0.4% of the requests for court orders were denied.


Germany

118 were considered relevant. The email contents were scanned for keywords relating to certain “areas of risk,” namely international terrorism, proliferation of arms and other military technology, and human smuggling.

The practice of German police authorities to make use of radio cell queries for criminal investigation on a regular basis has continued in the reporting period, and available data suggests a further increase to a significant degree. According to the response to an interpellation by the faction of the Pirate Party in the state parliament of Saarland, in that state alone there were more than 50 radio cell queries per day. In the state of Berlin however, in reaction to persistent criticism of the widespread practice, the state parliament enacted legislation in November 2014 that requires law enforcement agencies to inform cell phone users who are affected by a radio cell query via text. Furthermore, in the future the state is obligated to keep a public record of the practice.

After the European Court of Justice declared the EU Data Retention Directive to be unconstitutional on April 8, 2014, the EU Commission repeatedly announced that for the time being at least, it would abstain from proposing a new directive in line with the Court’s specifications. In reaction to this, however, several German politicians from the ruling coalition as well as representatives of the police union and members of the domestic intelligence services started calling for a German enactment of data retention. Federal Minister of Justice Maas and Federal Minister of the Interior de Maizière announced their joint legislative plan under a new name in April 2015. The draft has been criticized as being disproportionate and as violating the European Court of Justice’s guidelines. In particular, one news website revealed that under the new act, not only data received during phone calls would be preserved but continuing location data of cellphone users even absent incoming or outgoing calls. Moreover, an undisclosed collateral agreement to the legislation, leaked to the journalists at Netzpolitik.org, provided for the possibility for law enforcement to obtain stored data on a regular basis has continued in the reporting period, and available data suggests a further increase to a significant degree.

Note that the annually presented numbers do not refer to the last year but to the year before, i.e. 2013. The Parliamentary Control Panel periodically reports to the parliament and nominates the members of the G10 Commission. The G10 Commission controls surveillance measures and is also responsible for overseeing telecommunications measures undertaken on the basis of the Counterterrorism Act of 2002 and the Amendment Act of 2007.

These are aggregated figures related to the three areas of risk in which scanning took place according to the report of the Parliamentary Control Panel. Cf. Deutscher Bundestag, Drucksache 18/3709, January 8, 2015, 8. Note that the annually presented numbers do not refer to the last year but to the year before, i.e. 2013. The Parliamentary Control Panel periodically reports to the parliament and nominates the members of the G10 Commission. The G10 Commission controls surveillance measures and is also responsible for overseeing telecommunications measures undertaken on the basis of the Counterterrorism Act of 2002 and the Amendment Act of 2007.


142 These are aggregated figures related to the three areas of risk in which scanning took place according to the report of the Parliamentary Control Panel. Cf. Deutscher Bundestag, Drucksache 18/3709, January 8, 2015, 8. Note that the annually presented numbers do not refer to the last year but to the year before, i.e. 2013. The Parliamentary Control Panel periodically reports to the parliament and nominates the members of the G10 Commission. The G10 Commission controls surveillance measures and is also responsible for overseeing telecommunications measures undertaken on the basis of the Counterterrorism Act of 2002 and the Amendment Act of 2007.

144 Cf. the report of the Parliamentary Control Panel: Deutscher Bundestag, Drucksache 18/3709, January 8, 2015, 7.


147 Cf. the report of the Parliamentary Control Panel: Deutscher Bundestag, Drucksache 18/3709, January 8, 2015, 7.


Germany

information without the requirement of prior judicial authority. The federal government has since confirmed the existence of said agreement.

Intimidation and Violence

Aside from the case of alleged intimidating surveillance of a blogger reporting from the parliamentary inquiry commission concerning the NSA scandal as mentioned above, there have been no cases of direct intimidation of or violence against online journalists or other ICT users in the reporting period.

Technical Attacks

Human rights activists or non-governmental organizations are rarely victims of cyberattacks or other forms of technical violence that intend to intimidate or otherwise silence them. At the same time, cyberattacks have become an increasingly significant problem for industry in Germany. According to recent studies, almost one in three companies was affected by a substantial security breach in the past three years. However, investigations reveal that the majority of attacks are carried out by insiders, not through the internet. Moreover, small and medium-size companies are more prone to attacks than larger companies.

The annual financial damage has reached an estimated EUR 50 billion. The latest official cybersecurity report for Germany furthermore lists a particularly grave cyberattack against a steel mill in 2014, which led to the physical destruction of large parts of the facility.

In order to strengthen capabilities to react to cyberattacks, the Federal Ministry of the Interior proposed legislation to improve the security of information networks by obliging telecommunication firms and critical infrastructure operators to report security breaches to the Federal Office for Information Security (BSI). The bill was discussed in the committee for internal affairs of the Federal parliament in April 2015.

---


Hungary

### Key Developments: June 2014 – May 2015

- Following large protests in November 2014, the government decided to withdraw a proposal introducing a new tax that would have charged internet service providers per GB of data transferred, a fee which likely would have been passed on to consumers (see Availability and Ease of Access).

- In January 2015, a court ordered the blocking of an article from the far-right website Kuruc.info (see Blocking and Filtering).

- Internet access continues to expand in Hungary, reaching an internet penetration rate of 76 percent in 2014 (see Availability and Ease of Access).

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>24</td>
<td>24</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

<table>
<thead>
<tr>
<th>Population:</th>
<th>9.9 million</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Penetration 2014:</td>
<td>76 percent</td>
</tr>
<tr>
<td>Social Media/ICT Apps Blocked:</td>
<td>No</td>
</tr>
<tr>
<td>Political/Social Content Blocked:</td>
<td>No</td>
</tr>
<tr>
<td>Bloggers/ICT Users Arrested:</td>
<td>No</td>
</tr>
<tr>
<td>Press Freedom 2015 Status:</td>
<td>Partly Free</td>
</tr>
</tbody>
</table>

*0=most free, 100=least free
Introduction

Access to the internet in Hungary continues to expand, despite government policies and judicial decisions over the past few years that have threatened to impose restrictions on access and online content. In late October 2014, the Orban administration issued a proposal to tax internet service providers (ISPs) per gigabyte (GB) of data transferred. Many assumed that ISPs would pass on this fee to consumers, which could potentially inhibit or discourage users from accessing more data-heavy websites and applications. Following significant protests, the government withdrew the proposal, but signaled that it intended to revisit the issue later in 2015.

In the past, the government has refrained from blocking online content, other than illegal gambling websites, despite persistent calls to ban the far-right website Kuruc.info, a site that frequently features xenophobic, anti-Semitic, and other hate speech content. This year, a court issued an order to delete, or make “inaccessible,” an article on the website denying the Holocaust. Since the website is hosted on servers in the United States and the court could not force the deletion of the content, the court subsequently decided that the article should be blocked within Hungary.

Since 2010, the conservative Hungarian Civic Union (Fidesz) and its ally, the Christian Democratic People’s Party (KDNP) have executed a major overhaul of Hungarian legislation, including new laws regulating the media (including online media outlets and news portals) and new civil and penal codes, causing significant concern among civil liberties advocates and the international community more broadly. The established regulatory authority, the National Media and Infocommunications Authority (NMHH) and its decision-making body, the Media Council, were created to oversee the mass communications industry, with the power to penalize or suspend outlets that violate stipulations of the media regulations. In April 2011, the national assembly adopted a new constitution, the Fundamental Law of Hungary, which includes a provision concerning the supervision of the mass communications industry and the media as a whole. The parliament also created the National Agency for Data Protection, whose independence has been called into question due to the political appointment process of the agency’s leadership.

Immediately after the 2010 media laws were passed, Hungary came under fierce criticism from the international community, as the laws were deemed incompatible with the values of the European Union. Despite the modifications to the media laws in May 2012 based on the ruling of the Hungarian Constitutional Court in December 2011, members of the Organization for Security and Co-operation in Europe (OSCE) and the Council of Europe have argued that the laws remain unsatisfactory, and that unclear provisions and the significant power given to the NMHH continue to threaten media freedom. In January 2013, the Council of Europe welcomed the results of the dialogue with the Hungarian government about media regulation, while domestic nongovernmental organizations (NGOs) expressed their continued concerns to the Secretary General of the Council of Europe.

---

4 Council of Europe, ”Secretary General welcomes changes to Hungarian laws on media and judiciary,” news release, January 29, 2013, http://bit.ly/1LkX6hW.
Obstacles to Access

Access to the internet in Hungary is relatively free, with an internet penetration rate of over 75 percent. However, in late 2014 the Orban administration issued a controversial proposal to include an internet tax in the 2015 government budget, which would have charged internet service providers a small fee per gigabyte of data transferred. The proposal was withdrawn after large protests erupted over the issue. A national consultation was introduced online about the question of taxing internet use, and its results are intended to serve as a basis for recommendations for internet-related policy changes in September 2015.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), internet penetration in Hungary stood at over 76 percent in 2014, compared to 73 percent in 2013 and just 62 percent in 2009. The National Media and Infocommunications Authority of Hungary (NMHH) reported in December 2014 that there were over 2.4 million broadband internet subscriptions, in a country of less than 10 million inhabitants. According to a 2014 Eurobarometer survey, only 51 percent of Hungarian households had an internet connection.

Dial-up internet service is not widely used. The NMHH recorded a mobile phone penetration rate of about 117 percent and over 4.1 million mobile internet subscriptions in the past year. In 2014, only 22 percent of the population had never used the internet, a decrease from 52 percent in 2006. The Eurobarometer survey also found that 84 percent of Hungarian respondents considered price to be the most important factor when subscribing to an internet service provider (ISP).

There are geographical, socioeconomic, and ethnic differences in Hungary’s internet penetration levels, with lower access rates found among low-income families and in rural areas. According to the 2014 data from the TNS Hoffmann research company, internet penetration was over 82 percent among the employed but only 52 percent among those who were unemployed. Also, internet penetration differs between those living in the capital and in the countryside. There is no new data on the internet penetration level among the Roma community, the country’s largest ethnic minority, though in the past this group has had lower-than-average levels of internet access.

The National Core Curriculum for 2013 drastically decreased the number of IT classes in primary and
Hungary

secondary schools, despite protests from IT teachers, potentially further increasing the digital divide among social groups, as children coming from low-income families may not have access to computers and other digital devices in their homes. The poor IT infrastructure of public schools further increases the digital divide.

A proposed tax on internet usage in late 2014 sparked widespread protests in Hungary, which eventually led to the Orban administration’s withdrawal of the proposal. The tax would have involved charging ISPs approximately 150 forints (US$0.61) per GB of data, a fee which likely would have been passed on to consumers. During his speech withdrawing the proposal, Orban hinted at the possibility of reintroducing the idea of taxes and other regulations on the internet in early 2015, although so far no proposals have been formally introduced.

Restrictions on Connectivity

The government does not restrict bandwidth, routers, or switches, and backbone connections are owned by telecommunications companies rather than the state. Legally, however, the internet and other telecommunications services can be paused or limited in instances of unexpected attacks, for preemptive defense, or in states of emergency or national crisis. The Budapest Internet eXchange (BIX) is a network system that distributes Hungarian internet traffic among domestic internet service providers (ISPs), and is overseen by the Council of Hungarian Internet Service Providers (ISZT) without any governmental interference.

ICT Market

The ICT market in Hungary lacks significant competition, with over a third of the market belonging to Magyar Telekom. Three ISPs control over two-thirds of the total fixed broadband market. UPC was the first company to enable home routers to serve as Wi-Fi hotspots, at the same time entering the mobile phone market in the country. There are three mobile phone service providers, all privately owned by foreign companies. The existence of only three mobile phone service providers (in

18 Zoltán Kalmár, Council of Hungarian Internet Service Providers, e-mail communication, January 24, 2012.
20 Act CXIII of 2011 on home defense, Military of Hungary, and the implementable measures under special legal order, Art. 68, par. 5.
22 Zoltán Kalmár, Council of Hungarian Internet Service Providers, email communication, January 24, 2012.
23 These major internet service providers are: Telekom with a 35.8 percent market share, UPC 21.9 percent, and DIGI 14.2 percent. See National Media and Infocommunications Authority Hungary, Flash report on landline service, December 2014, http://bit.ly/1a9XYXp.
25 The three mobile phone companies are: Telekom with a 46.82 percent market share, Telenor 30.48 percent, and Vodafone 22.7 percent. See National Media and Infocommunications Authority Hungary, Flash report on mobile internet, January 2014, http://bit.ly/1VJbhK.
addition to the resellers that use the networks of the three major mobile phone service providers) has created a relatively stagnant market in terms of mobile internet network expansion.

The government levied two special taxes on the telecommunication industry in 2010, both of which triggered infringement proceedings in the European Union in 2012. Both proceedings were ultimately withdrawn,\(^{26}\) and the government withdrew the special tax levied in 2010. To counterbalance the budgetary loss, another tax was introduced in mid-2012 on mobile phone calls and text messages (a maximum of $3 monthly for individual subscribers).\(^{27}\) All mobile service providers have since raised their prices.\(^{28}\)

**Regulatory Bodies**

The National Media and Infocommunications Authority of Hungary (NMHH) and the Media Council, established under the 2010 media laws, are responsible for overseeing and regulating the mass communications industry. The Media Council is the NMHH’s decision-making body in matters related to media outlets, and its responsibilities include allocating television and radio frequencies and penalizing violators of media regulations. The members of the Media Council are nominated and elected by the parliamentary majority.\(^{29}\) Based on consultations with industry leaders and the Council of Europe in January 2013, the nomination process was amended, after which the president of the NMHH (and president of the Media Council if elected by the parliamentary majority) is no longer appointed directly by the prime minister but by the president of the republic, based on the proposal of the prime minister, for a non-renewable nine-year term.\(^{30}\)

Despite these modifications, some of the decisions of the Media Council have been regarded as politicized. For instance, Mérték Media Monitor revealed in several analyses that during the radio frequency allocation processes, preference was given to only a few applicants, who received a large share of the available frequencies.\(^{31}\)

With the adoption of the Fundamental Law of Hungary, which entered into force in January 2012, the governing parties prematurely ended the six-year term of the well-functioning Data Protection Commissioner, replacing the former office with the National Agency for Data Protection. The head of the new agency is appointed by the president of the republic based on the suggestion of the prime minister for a nine-year term and can be dismissed by the president based on the suggestion of the prime minister on potentially arbitrary grounds,\(^{32}\) calling into question the independence of the agency. In 2014, the Court of Justice of the European Union ruled that Hungary failed to fulfill its obligations derived from EU law due to the early termination of the term of the Data Protection Commissioner.\(^{33}\)


\(^{29}\) Act CLXXXV of 2010, art. 124.

\(^{30}\) Act CLXXXV of 2010, art. 111/A.


\(^{32}\) Act CXII of 2011 on data protection and freedom of information, Section 40, par. 1, 3; Section 45, par. 4–5.

\(^{33}\) Case C-288/12, Commission v Hungary, April 8, 2014.
Hungary

Limits on Content

Over the past few years, revisions to the civil and criminal codes have somewhat altered the regulatory landscape when it comes to online content, including revisions to the penal code in 2013 requiring ISPs to block illegal content if the content is hosted outside of Hungary (meaning the servers are outside Hungarian jurisdiction and the courts cannot force the deletion of the content). There is no sign of the government mandating any systematic filtering of websites, blogs, or text messages, though in 2015 a Hungarian court ordered the deletion of an article based on the new penal code. Online content is somewhat limited as a result of self-censorship, lack of revenue for independent media outlets online, the dominance of the state-run media outlet, and the biased nature of the allocation of state advertisement funds.

Blocking and Filtering

The government does not place any restrictions on access to social media or communication applications. YouTube, Facebook, Twitter, Tumblr, international blog-hosting services, instant messaging, person-to-person communication, and other applications are freely available.

In January 2015, the Metropolitan Court of Justice ordered the far-right website Kuruc.info to delete an article denying the Holocaust. The stipulation of the penal code is often called the “Kuruc.info law” by experts, as the law was largely drafted to target the infamous website, which is hosted abroad. Since the website is hosted outside of Hungarian jurisdiction and therefore cannot be forced to shut down, the prosecutors of district V and XIII of Budapest stated that the article on Kuruc.info would be permanently blocked in May 2015, though the article was still accessible as of June 2015.

The new penal code, which took effect on July 1, 2013, includes provisions based on which websites can now be blocked in cases of unlawful online content. The law stipulates that if the illegal content is hosted on a server located outside of the country, the Hungarian court will issue a query to the Minister of Justice to make the electronic content inaccessible; the minister then passes the query onto the “foreign state,” and if there is no response from that state for 30 days, the court can order domestic ISPs to make the given content inaccessible. The NMHH is the authority designated to manage the list of websites to be blocked based on court orders (or the tax authority in case of illegal gambling), while the operation of the system is regulated by a decree of the NMHH, which enables the authority to oblige ISPs to block the unlawful content.

38 Act C of 2012, art. 77.
39 Act XXXVIII of 1996 on International Assistance in Criminal Matters, art. 60/H.
40 Act C of 2003 on electronic communication, art. 10, par. 28., art. 159/B.
(Hungarian acronym for “central electronic database of decrees on inaccessibility”), went into effect on January 1, 2014 with the primary aim of fighting child pornography. However, the blacklist is not public, as only certain institutions (such as the courts, parliamentary committees, the police, etc.) have access to the list of blocked websites.

Online gambling is considered an illegal activity if the tax authority has not authorized the operation of the website. 42 ISPs had blocked 69 gambling websites as of June 2015; 43 however, gambling websites have been known to change their URLs in order to circumvent the blocking system. 44

**Content Removal**

Intermediaries are not legally responsible for transmitted content if they did not initiate or select the receiver of the transmission, or select or modify the transmitted information. 45 Intermediaries are also not obliged to verify the content they transmit, store, or make available, nor do they need to search for unlawful activity. 46 Hosting providers are required to make data inaccessible, either temporarily or permanently, once they receive a court order stating that the hosted content is illegal. 47

Nevertheless, the 2010 media laws contain several general content regulation provisions concerning online media outlets, particularly if these outlets provide services for a profit. For example, the media regulation states that print and online media outlets bear editorial responsibility if their aim is to distribute content to the public for “information, entertainment or training purposes,” but that editorial responsibility “does not necessarily imply legal liability in relation to printed press materials.” 48 The law fails to clarify what editorial responsibility entails and whether it would imply legal liability for online publications. A member of the Media Council claimed that this provision could apply to a blog if the blog were produced for a living. 49 According to László Bodolai, a lawyer for the news outlet Index.hu and a media law expert, based on a 2015 court decision, bloggers cannot legally be forced to amend or correct content with which someone disagrees; however, lawsuits and damnification fees can apply. 50

In June 2012, the Supreme Court condemned the publishers of two blogs for defamation committed in comments posted on their sites, regardless of the fact that the comments had been deleted. The Supreme Court ruled that the plaintiff’s reputation was harmed, and that the defendants needed to pay for the legal expenses incurred, even though they were not the original authors of the comments. 51

The implications for legal liability for comments posted online were further substantiated by a judgment of the Constitutional Court in 2014. In May 2014, the Constitutional Court issued a ruling

---

42 Act XXXIV of 1991 on Gambling, art. 36/g.
43 The list of the National Tax and Customs Administration can be accessed at: http://en.nav.gov.hu/.
45 Act CVIII of 2001 on Electronic Commerce, art. 8, par. 1.
46 Act CVIII of 2001, art. 7. par. 3.
47 Act CVII of 1998 on criminal proceedings, art. 158/B-158/D.
48 Act CIV of 2010, art. 1, par. 6.
50 László Bodolai, personal communication, March 2, 2015.
stating that the publisher bears responsibility for comments posted on a given website.52 Dunja Mijatovic, the OSCE Representative on Freedom of the Media warned that the judgment may curb freedom of expression.53 Similarly, on October 10, 2013, the European Court of Human Rights upheld a decision by the Estonian Supreme Court that ruled that web portals are responsible for all comments posted to their sites. However, the implications of this European decision have yet to be clarified in Hungary.54 According to László Bodolai, the courts’ rulings shows that if a comment is posted below an article (i.e., edited content), then it might be considered unlawful, but if the comment is posted on a forum, then it cannot be considered unlawful.55

The 2010 media laws stipulate that media content—both online and offline—may not offend, discriminate or “incite hatred against persons, nations, communities, national, ethnic, linguistic and other minorities or any majority as well as any church or religious groups.”56 Further, the law states that constitutional order and human rights must be respected, and that public morals cannot be violated.57 However, the law does not define the meaning of “any majority” or “public morals.” If a media outlet does not comply with the law, the Media Council may oblige it to “discontinue its unlawful conduct,” publish a notice of the resolution on its front page, and/or pay a fine of up to HUF 25 million (approximately $93,000).58 If a site repeatedly violates the stipulations of the media regulation, ISPs can be obliged to suspend the site’s given domain, and as a last resort, the media authority can delete the site from the administrative registry.59 Any such action can be appealed in court, although the 2011 overhaul of the judiciary calls into question the independence of the court system.

Media, Diversity, and Content Manipulation

The online media environment in Hungary is relatively diverse, though there are financial concerns regarding the allocation of advertising and political pressures to self-censor with regard to certain topics.

A series of interviews conducted among journalists in 2014 by Mérték Media Monitor revealed the persistence of self-censorship in Hungary due to political and economic pressures. Over 50 percent of the respondents reported experiencing restraints on press freedom due to political and economic pressure. They further reported these pressures tend “to manifest themselves in requests to conceal certain issues or names, or to compile their reports in a way that fails to properly reflect reality,” with 30 percent of respondents reportedly practicing self-censorship to avoid consequences at work.60 The report notes that pressure is exerted by members of the elite political class and oligarchs “cracking down” on independent journalism efforts with a variety of tools, such as changes in ownership structure, financial and political pressure, and official and legal instruments.61

55 László Bodolai, personal communication, March 2, 2015.
56 Act CIV of 2010, art. 17.
57 Act CIV of 2010, art. 16, and art. 4, par. 3.
58 Act CLXXXV of 2010, art. 186, par. 1, 187, par. 3. bf.
59 Act CLXXXV of 2010, art. 187, par. 3. e, 189, par. 4.
Soon after the 2010 parliamentary elections, state advertising funds were partially or completely withdrawn from some newspapers, allegedly for political reasons, while others multiplied their revenues from such state sources. Additionally, private advertisers tend to advertise where state companies do, meaning that some media outlets (those generally critical of the government) are “bleeding out.” The concentration of state advertisement spending further increased for 2015, with the internet being the only exception, where the trend of biased distribution of state advertisement funds is not visible. There is currently no comprehensive data to determine the level of political influence over advertisements in cases of online media specifically. Stop.hu, a website close to the opposition Socialist party, was forced to start making reductions in staff in July 2013 partly due to the fact that, according to the manager, many businesses would not consider advertising on their site because the content is critical of the government.

In June 2014, Gergo Saling, the editor-in-chief of the online media outlet Origo.hu, was dismissed following the publication of a series of articles critical of the government, including one that revealed a possible abuse of public funds by the undersecretary of the prime minister. The dismissal raised suspicions that the government, which has extensive ties to Deutsche Telekom, the owner of Origo.hu through the subsidiary Magyar Telekom (MT), had pressured the parent company to fire the editor. The news outlet 444.hu reported that the Hungarian government asked Magyar Telekom to “either reign in Origo or let it go.” Following Saling’s termination, several members of the editorial board resigned in protest. Origo.hu announced that the editor-in-chief left the company through a mutual agreement.

The introduction of the advertisement tax, which media outlets pay based on their revenues from advertisement, is also a burden for some media outlets, particularly smaller online media ventures. In May 2015, the tax was converted from a progressive tax into a flat tax, as the European Commission started investigating whether the tax harms competition rules.

Despite reports of self-censorship and the challenge of maintaining financial viability, online media outlets have become a tool to scrutinize public officials. For instance, starting in January 2012, Hvg.hu, an online news portal whose content is mostly separate from the printed business weekly HVG, published a series of articles on how the then-president of the republic plagiarized his doctoral dissertation. Although he denied any wrongdoing, Pál Schmitt resigned in April 2012. Some online media outlets, particularly Atlatszo.hu, have made repeated requests for public data from public...
institutions for the purposes of investigative reporting. This independent media outlet has continuously published lists of public fund misuse by politicians, though such efforts have resulted in few consequences given the publication’s limited reach.72

Since 2011, the state-owned Hungarian News Agency (MTI) has had a virtual monopoly on the news market, as media outlets that have been impacted by the economic crisis tend to republish MTI news items, most of which are available to other news outlets free of charge. During its overhaul, MTI became integrated into the system of public service broadcasting, led by the media authority. The media laws oblige MTI to produce news bulletins for public service broadcasters and edit their joint news portal.73 In late 2014, due to yet another modification of the media laws, the state media became further centralized, as the public service radio and television (both MTV and Duna TV) and MTI merged into the entity of Duna TV.74 An analysis of the Hungarian public service broadcasters’ news bulletins in 2013 indicated that they “tend to select and to frame the news in a way that is favorable to the incumbent center-right government.”75

Although MTI has a major effect on traditional and online content, the online media landscape is still relatively diverse. Most civil society organizations have websites, and an increasing number of them have a presence on Facebook. There are some media outlets, including online portals, representing the minority Roma community,76 the LGBTI community, and religious groups. Nevertheless, many news sources, although independent, often reflect the politically-divided nature of Hungarian society, and partisan journalism is widespread.

Blogs are generally considered an opinion genre and do not typically express independent or balanced news. There are also blogs analyzing governmental policies, the activities of public figures, and corruption. Trolling is usually moderated in the comments sections of articles, typically to prevent negative discussions. It was reported that politicians have used pseudonyms to participate in online forum discussions, and parties and ministries have implemented a monitoring system to be able to participate in discussions related to their work.77 A survey conducted in 2011 among those netizens who knew what “commenting” meant indicated that 87 percent of the respondents encountered trolling on websites, but an overwhelming majority of the respondents considered commenting as a form of freedom of expression.78

Digital Activism

Social media platforms such as Facebook, which had almost 4.6 million users in Hungary as of March 2015, have grown increasingly popular as a tool for advocacy, especially after the 2010 parliamentary elections.79 Since then, several large demonstrations have been organized through Facebook, mobi-

72 Tamás Bodoky, the founder of Atlatszo.hu and the portal itself got nominated with four other initiatives globally by Index on Censorship Freedom of Expression awards in category of Digital Activism in 2015, Index, “Digital Activism Nominees 2015,” http://bit.ly/1GCEDZI.
73 Act CLXXXV of 2010, art. 101, par. 4.
74 Act CLXXXV of 2010, art. 215/A.
lizing tens of thousands of people. In 2014, there were protests organized online for various social and political issues, the largest of which drew thousands of people to protest against the introduction of a tax on internet use. Due to the overwhelming demonstrations, the government decided to withdraw the planned tax.

Violations of User Rights

The right to freedom of expression is protected in the Fundamental Law of Hungary, and the government does not generally prosecute individuals for posting controversial political or social content online. However, the law includes criminal penalties for defamation, and new amendments in November 2013 added criminal penalties for disseminating defamatory video or audio content. Judicial oversight of surveillance by intelligence agencies continues to be a concern, given that surveillance is authorized by the justice minister rather than through a court warrant.

Legal Environment

The Fundamental Law of Hungary acknowledges the right to freedom of expression and defends “freedom and diversity of the press,” although there are no laws that specifically protect online modes of expression. In 2012, the European Commission launched several infringement proceedings against Hungary. The European Commission expressed concerns over Hungary’s decision to lower the mandatory retirement age from 70 years to 62 years for judges and prosecutors, effectively sending 274 judges, including some on the Supreme Court, into early retirement. In November 2012, the Court of Justice of the European Union ruled that the early retirement of judges, prosecutors, and notaries was discriminatory. Prior to that, in July 2012, the Hungarian Constitutional Court ruled that the early retirement provision was unconstitutional. In March 2013, the parliament accepted a law that gradually decreases the retirement age of judges, prosecutors, and pensioners from 70 to 65 over the next 10 years.

On November 5, 2013, the criminal code was modified to include prison sentences for defamatory video or audio content. Anyone creating such a video can be punished by up to one year in prison, while anyone publishing such a recording can be punished by up to two years. If the video is published on a platform with a wide audience or in some way causes significant harm, the sentence can increase to up to three years in prison. The amendment was condemned both by domestic and

83 "European Commission launches accelerated infringement proceedings against Hungary over the independence of its central bank and data protection authorities as well as over measures affecting the judiciary" European Commission.
84 Judgment of the Court (First Chamber), Case C-286/12, November 6, 2012, [link](http://bit.ly/14TuyKJ).
85 "Elkaszálták a bírói nyugdíjszabályt," [The retirement rule for judges was annulled] Index, July 16, 2013, [link](http://bit.ly/1OpXIUc).
86 "Meggazdították a bírálás lassú nyugdíjszabályát," [The law on the slow retirement of judges was accepted] Hvg.hu, March 11, 2013, [link](http://bit.ly/1PkJOSb).
87 Act C of 2012, art. 226/A and 226/B.
Hungary

international actors for threatening freedom of expression and for targeting the media, given that the longest sentence applies to materials that are widely published.

In May 2013, the parliamentary majority modified the freedom of information act to restrict the accessibility of public data, claiming that some of the requests were “excessive.” The president vetoed the bill, after which the draft was amended partly based on the suggestions of the head of the Hungarian National Authority for Data Protection and Freedom of Information. The amended law was passed and came into effect on June 21, 2013; however, the law remains ambiguous and leaves the potential for requests for information to be denied arbitrarily. According to the law, the data holders themselves can decide to reject requests that are “overarching,” “invoice-based,” or “itemized.” The law does not define what these terms mean, leaving it up to the data holder authority to make this determination.

Critics of the 2010 media laws contend that the Media Council operates with unclear provisions and imposes high fines and sanctions on media outlets, which might give rise to uncertainty and fear, lead to self-censorship, and have a chilling effect on journalism as a whole. In December 2011, the Constitutional Court struck down several provisions applicable to print and online outlets “but without touching on the organizational frames and system of supervision.” In May 2012, the parliament modified the media regulation, ostensibly in order to comply with the ruling of the Constitutional Court, but left the provisions regarding high fines and the problematic nominating process for members of the Media Council. OSCE Representative on Freedom of the Media Dunja Mijatovic warned that the amendments “only add to the existing concerns over the curbing of critical or differing views in the country.”

Hungarian law does not distinguish between traditional and online media outlets in libel or defamation cases, and the criminal code stipulates that if slander is committed “before the public at large,” it can be punished by imprisonment of up to one year. The criminal code bans defamation, slander, the humiliation of national symbols (the anthem, flag, and coat of arms), the dissemination of totalitarian symbols (the swastika and red pentagram), the denial of the sins of national socialism or communism, and public scare-mongering through the media. However, in February 2013, the Constitutional Court ruled the ban on using totalitarian symbols unconstitutional, though the parliamentary majority decided to include it again in revisions to the penal code in April 2013.

90 Act CXII of 2011 on informational self-determination and freedom of information.
98 Act C of 2012, art. 227.
100 “Constitutional Court voids ban on “symbols of tyranny”; red star, swastika to become legal on April 30;”, Politics, February
The new civil code, which took effect in March 2014, recognizes civil rights (including protection against defamation) and bans the insulting of an individual's honor,\(^{101}\) and includes a damnification fee for non-pecuniary damages caused by violating civil rights.\(^{102}\) Libel cases demonstrate that the courts generally protect freedom of expression, except when there is a conflict with another basic right. Defamation cases have decreased since a 1994 Constitutional Court decision, which asserted that a public figure's tolerance of criticism should be higher than an ordinary citizen's.\(^{103}\) However, the new civil code includes a provision that may limit the free discussion of public affairs in cases where the human dignity of a public figure is violated.\(^{104}\) Some fear that the provisions of the new civil code could result in a slew of slander and libel cases initiated by anyone, including public figures, who can claim that their dignity has been harmed.

Another debated issue is related to a provision in the new civil code, which went into effect in March 2014, stipulating that a photographer must obtain permission from the subjects in the picture when taking press photos (except at public events).\(^{105}\) Industry experts argue that the law is too vague and obstructs the profession of photojournalism, while the code's proponents claim that this stipulation merely confirms the courts' practice.\(^{106}\) The ministry explains consent might happen with "implicit behavior," such as someone not objecting with waiving his or her hands. It is unclear how the judiciary will interpret and apply this new provision, which could impact online and citizen journalists' ability to document newsworthy events; many judges themselves have stated that they do not know how to rule on such cases.\(^{107}\) Nevertheless, in September 2014, the Constitutional Court ruled that the law does not require media outlets to blur the faces of police officers in photographs, reversing a practice that had been required since 2007.\(^{108}\)

### Prosecutions and Detentions for Online Activities

As of May 2015, no online media outlet had been penalized for violating the new stipulations introduced by the 2010 media laws, except for a case in early 2013 in which a blogger received a suspended sentence on charges of incitement to violence.\(^{109}\)

Prior to 2008, the penal code was rarely used in cases of defamation or slander.\(^{110}\) However, criminal investigations of online activities are a growing phenomenon. In November 2012, the police launched an investigation based on comments that appeared on Nepszava.hu\(^{111}\) and the news site

\(^{101}\) Act V of 2013 on the Civil Code, art. 2:45.

\(^{102}\) Act V of 2013 on the Civil Code, art. 2:52–53.


\(^{104}\) Bill Nr. T/7971, art. 2:44.

\(^{105}\) Act V of 2013 on the civil code, art. 2:48.


Hungary

Hir24.hu\(^{112}\) that criticized Ferenc Papcsák, a former Fidesz member of parliament and mayor of a district in Budapest. The police ordered the release of the personal data connected to these comments, including the users’ internet protocol (IP) and email addresses, although in the case of the latter site, commenters log-in via Facebook rather than providing a username or email address.

In another case involving online libel, an article was published in October 2012 on Delmagyar.hu—the online version of the regional daily Délmagyarország—about a lethal car accident involving János Lázár, a Fidesz member of parliament (MP). Lázár claimed that some of the comments left on the online article were an affront to his human dignity. Though the editorial board removed the comments in question, the MP launched a libel case based on the penal code as well as a civil proceeding against the publisher to claim compensation for the non-pecuniary damages caused.\(^{113}\) In July 2013, the publisher was ordered to pay HUF 500,000 (approximately US$2,220) as compensation to Mr. Lázár based on an out-of-court settlement,\(^{114}\) while the penal proceeding was withdrawn by Lázár in 2014.\(^{115}\)

In December 2014, the local council of the town of Tata announced that it intended to sue a Facebook commenter who claimed the council was misusing public funds, and that it would sue all other commenters sharing or commenting on the original commenter’s post.\(^{116}\) To date, no proceedings have been filed regarding this case.

In January 2013, a blogger named Tamás Polgár, alias “Tomcat,” was condemned for incitement and received a suspended prison sentence of one year and two months based on the penal code\(^{117}\) for a 2009 blog post in which he called upon readers to “beat up Gypsies,” during a time when six Roma people had been killed in a case of serial murders.\(^{118}\) This was the first case since the democratic transition in which someone had been prosecuted under the penal code for material they posted online. The sentence was suspended for five years, and in June 2013, a judge modified the penalty to 50 days of community service.\(^{119}\)

Surveillance, Privacy, and Anonymity

The lack of judicial oversight for surveillance of ICTs, combined with the evidence revealing that the Hungarian government has purchased invasive surveillance technologies from Hacking Team and other companies, raises concerns about the degree to which the right to privacy online is fully protected.


\(^{117}\) Act IV of 1978, Article 269 says: “A person who incites to hatred before the general public against a) the Hungarian nation, b) any national, ethnic, racial group or certain groups of the population, shall be punishable for a felony offense with imprisonment up to three years.”


Hungary

Generally, users who wish to comment on a web article need to register with the website by providing an email address and username, or they need to use a Facebook login. The operator of a website may be asked to provide the authorities with a commenter’s IP address, email address, or other data in case of an investigation. Additionally, to sign a contract with a mobile phone company, users must provide personal data upon purchase of a SIM card. Encryption software is freely available without government interference; Pretty Good Privacy (PGP), a data encryption program, is used by investigative journalists.

National security services can "gather information from telecommunications systems and other data storage devices" without a warrant. The authorities have allegedly installed black boxes on ISP networks. Secret services can access and record communication transmitted via ICTs, though a warrant is required. There is no data on the extent to which, or how regularly, the authorities monitor ICTs. In June 2012, staff of the Eötvös Károly Institute (EKINT) issued a complaint to the Constitutional Court requesting the annulment of the provision that allows the justice minister overseeing the work of the Counter Terrorism Center to approve the secret surveillance of individuals. They argued against the constitutionality of the provision and that such surveillance should be tied to the approval of a judge rather than a minister. The Constitutional Court rejected the complaint, after which EKINT addressed a complaint to the European Court of Human Rights in May 2014. The application was joined by Privacy International and the Center for Democracy & Technology. As of May 2015, the case is still pending before the court.

Over the past few years, several privacy and digital rights organizations have pointed to evidence that the Hungarian authorities have purchased potentially invasive surveillance technologies. In 2013, Privacy International reported that Hungarian law enforcement agencies are connected with at least one surveillance technology company, and that several government agencies attended the ISS World surveillance trade shows over the years. Citizen Lab also reported finding a FinFisher Command and Control server in Hungary, though it was not clear whether the server is operated by the government or other actors. In July 2015, files leaked from the information technology company Hacking Team revealed that the Hungarian government was a client.

According to the Electronic Communications Act, electronic communications service providers are

---

120 Act XIX of 1998 on criminal proceedings, art. 178/A, par. 1.
125 Act CXXV of 1995, art. 56.
126 Act CXXV of 1995, art. 58, par. 2. states that in some instances – basically including the tasks of the Counter Terrorism Center – the minister for justice can grant the warrant.
127 The complaint can be downloaded at: http://ekint.org/ekint_files/File/constitutionalcomplaint_tek.pdf.
133 Electronic service providers provide electronic communications service, which means a “service normally provided against remuneration, which consists wholly or mainly in the conveyance, and if applicable routing of signals on electronic communications networks, but exclude services providing or exercising editorial control over the content transmitted using

---
Hungary

obligated to “cooperate with organizations authorized to perform intelligence information gathering and covert acquisition of data.” Additionally, the act states that “the service provider shall, upon the written request from the National Security Special Service, agree with the National Security Special Service about the conditions of the use of tools and methods for the covert acquisition of information and covert acquisition of data.”

In accordance with the EU Directive 2006/24/EC on data retention, ISPs and mobile phone companies in Hungary must retain user data for up to one year, including personal data, location information, phone numbers, the duration of phone conversations, IP addresses, and user IDs for investigative authorities and security services. There is no data on the extent of these activities, even though there is a legal obligation to provide the European Commission with statistics on the data queries made by investigating authorities. However, in April 2014, the European Court of Justice declared the EU Data Retention Directive invalid, causing a number of countries within the EU to rethink their data retention legislation. In October 2014, the Hungarian Civil Liberties Union launched litigation against two of the major mobile phone providers in an attempt to force the Hungarian Constitutional Court to withdraw its law on data retention.

Intimidation and Violence

Bloggers, ordinary ICT users, websites, or users’ property are not generally subject to extralegal intimidation or physical violence by state authorities or any other actors. In October 2012, there was one physical attack against a journalist from Index.hu, whose nose was broken by an extreme-right protester at an anti-government rally.

Technical Attacks

There were no significant cyberattacks against NGO websites or news outlets during the coverage period. In the past, technical attacks in Hungary have been primarily perpetrated by non-state actors against government websites, particularly by the international group Anonymous. For instance, in 2012 the group rewrote the text of the fundamental law on the website of the Constitutional Court, and several sites suffered from DDoS attacks during that time.

---

134 Act C of 2003, art. 92, par. 1.
135 Act C of 2003, art. 92, par. 2.
137 Act C of 2003, art. 159/A, par. 7.
Iceland

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 328,000

Internet Penetration 2014: 98 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: No

Bloggers/ICT Users Arrested: No

Press Freedom 2015 Status: Free

Key Developments: June 2014 – May 2015

- Iceland continues to have one of the highest rates of internet access in the world, with an internet penetration rate of 98 percent in 2014 (see Availability and Ease of Access).

- A resolution on the protection of user rights was adopted by the parliament in 2014 and awaits implementation; several bills on whistleblower protection and data retention were also presented in parliament in March 2015 (see Legal Environment).
Iceland

Introduction

Iceland has some of the highest rates of internet and social media use in the world, according to the World Economic Forum. Internet and digital media play a vital role in Icelandic society, and Iceland is an international leader when it comes to focusing on free speech and online media. The “crowdsourced constitution” process continues, following in the wake of the country’s financial collapse in 2008 when the three major banks went bankrupt, and social media platforms such as Facebook were integrated into the process of creating a new constitution. In June 2010, the Icelandic parliament launched a new media initiative protecting free speech, aiming to make Iceland a safe haven for journalists and whistleblowers. In March 2015, a series of bills on data retention and whistleblower protection, among other things, were presented in the parliament. In addition, a parliamentary resolution concerning the benefits of a free and unrestricted internet and the protection of user rights was adopted in late 2014 and awaits implementation in the near future.

Obstacles to Access

Iceland is one of the most connected countries in the world, with the highest percentage of households with access to the internet in Europe. There are very few obstacles to accessing the internet; however, the ICT regulatory agency’s ability to address concerns about concentration in the market has been limited. In 2013, the government passed legislation to address this issue, allowing the Competition Authority some oversight powers with regard to regulating media concentration.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), Iceland had an internet penetration rate of nearly 98 percent in 2014, compared to 97 percent in 2013 and 93 percent in 2009, with only a minimal difference in usage between the capital region and the other regions of the country. This is the highest percentage of internet users of all European countries, compared to an average internet penetration rate of 81 percent within the European Union.

Broadband connections were put into operation in 1998, and by 2006, slightly less than 90 percent of Icelandic households had internet access. The percentage of households with high speed internet connections, such as ADSL or SDSL, has increased greatly in recent years. In 2007, the Icelandic city of Seltjarnes became the first municipality in the world where every citizen has access to fiber-optic internet service.

References:
2. Email interview with employee at the Prime Minister’s Office, April 27, 2015.
4. International Modern Media Institute (IMMI), https://immi.is/
7. Statistics Iceland, http://www.statice.is
Iceland

The price of accessing the internet via computers and mobile phones is very affordable: a basic internet subscription with 5 GB of data costs around ISK 3,744 per month (approximately US$27), and a basic mobile phone connection with 500 Mb of data costs around ISK 681 per month (approximately US$5),\(^\text{11}\) while the average monthly salary is approximately ISK 464,000 (US$3,420).

Icelanders are frequent internet users, with 95 percent connecting to the internet daily or almost daily.\(^\text{12}\) A vast majority of the population (78 percent) is connected via broadband, and a growing number (22 percent) are connected via fiber-optics.\(^\text{13}\) In addition, 82 percent of Icelanders had access to the internet via a mobile connection in 2014.\(^\text{14}\) Furthermore, 84 percent of individuals used social networks, 95 percent read news online, 95 percent sent or received emails, 93 percent used online banking, and 34 percent stored electronic content on internet storage space.\(^\text{15}\)

Restrictions on Connectivity

There are no government-imposed restrictions on connectivity in Iceland. The country has been connected to the internet since 1989 via the NORDUnet in Denmark. The following year, a leased line to NORDUnet in Sweden was established, and the link was gradually upgraded. The Nordic connection was supplemented in 1997, when ISnet established a direct connection to Teleglobe in Canada, which was upgraded when the line was moved to New York in 1999.\(^\text{16}\)

Iceland has multiple channels connecting the country to the international internet, including connections to the international backbone through three submarine cables: FARICE-1, DANICE, and Greenland Connect. The Reykjavik Internet Exchange Point (IXP), which exchanges internet traffic among internet service providers (ISPs) located in Iceland, is operated independently of the government by the top-level domain registry ISNIC.

ICT Market

Síminn is the main internet and telecommunications operator in Iceland and runs fixed-line and mobile voice call services, as well as internet services and broadband television. Síminn is based on a merger between Landssími Islands, which was privatized in 2005, and the company Skipti ehf. Of the ISPs in Iceland, Síminn holds the largest market share (52.3 percent), followed by Vodafone (30 percent), Tal (7.9 percent), and Hringdu (3.6 percent), with the other companies comprising the remaining 6.2 percent. Regarding market share in mobile broadband, Síminn is the leading provider with the largest market share (42.9 percent), followed by Nova (30.1 percent), Vodafone (25.5 percent), and Tal (1.3 percent).\(^\text{17}\)

\(^\text{14}\) Statistics Iceland, [http://www.statice.is](http://www.statice.is)
\(^\text{15}\) Statistics Iceland.
\(^\text{17}\) The Post and Telecom Administration, "Statistics on the Icelandic Electronic Communications Market for the First Half of 2014."
Iceland

Regulatory Bodies

The main regulatory body governing information and communication technologies (ICTs) in Iceland is the Post and Telecom Affairs (PTA), which is an independent center under the direction of the Ministry of the Interior. The PTA supervises development, logistics, and fair competition in the field of telecommunications networks. Decisions of the PTA may be referred to the Rulings Committee for Electronic Communications and Postal Affairs. The Minister of the Interior appoints the three members of the Appellate Committee, following the nomination by the Supreme Court. The chairman and vice chairman must comply with the competence qualifications applying to Supreme Court judges. The members of the committee are appointed for a period of four years.\(^18\) In addition to the PTA, the Ministry of the Interior is responsible for the legal matters relating to online content.

A new media law, established on September 1, 2011, continued to stir debate in subsequent years.\(^19\) While the intention of the law was to create greater press freedom through a comprehensive framework governing broadcast, press, and online media, it also established an oversight body, the State Media Commission. According to the law, the Minister of Education, Science and Culture appoints five people to the Media Commission for terms of four years at a time. Two representatives are appointed in accordance with a nomination by the Supreme Court, one in accordance with a nomination by the standing Committee of Rectors of Icelandic Higher Education Institutions, and one in accordance with a nomination by the National Union of Icelandic Journalists. The fifth member is appointed by the minister without an outside nomination.\(^20\)

The Media Commission has no authority to deal with media concentration issues (a major concern of public debate in Iceland), but new legislation was put forth in 2013 that would give the Competition Authority oversight responsibility in consultation with the Media Commission. The bill was passed as an amendment to the new media law in March 2013. The amendment gives the Competition Authority other means and measures to deal with competition cases when media companies are concerned. Thus, the Competition Authority can look at issues such as plurality and whether there will be a decrease in newsrooms resulting from mergers and acquisitions, for example. According to the bill, the Media Commission shall in such cases give its opinion from a media authority’s perspective.\(^21\)

In July 2014, the Prime Minister appointed a working group to review the laws, regulations and administrations of regulatory authorities and evaluate how principles of good regulations and practices are met. In September 2014, the Minister for Education, Science and Culture is set to research the feasibility of the merger of four regulatory authorities: the Media Commission, the Post and Telecom Administration, the Icelandic Competition Authority, and the monitoring part of the National Energy Authority in Iceland. Recommendations will be published in the end of May 2015.\(^22\)

Limits on Content

Access to information and online communication is generally free from government interference; however, in October 2014 a court ordered online content to be blocked for the first time, in a case involving

---

19 Email interview with former employee at the Icelandic Media Commission, Jan 29, 2014.
21 Fjolmidlanefnd, “The Media Commission.”
22 Email interview member of the Media Commission, April 29, 2015.
Iceland

two BitTorrent websites. Iceland is not a member of the European Union, although the country is part of the European Economic Area and has agreed to follow legislation regarding consumer protection and business law similar to other member states.23

Blocking and Filtering

In October 2014, the Reykjavik District Court ordered two ISPs (Hringdu and Vodafone) to block the file-sharing website The Pirate Bay and the largest private Icelandic torrent website, Dei1du. The court order came after the music rights group STEF and the motion picture association SMAIS attempted to have the file sharing websites blocked due to copyright infringement, since much on the content on these sites is pirated material. In 2013, the two groups reported the torrent websites to the police. In May 2014, the Supreme Court declared that only one of the groups (STEF) could claim the injunctive relief right.24

Prior to the blocking, in April 2013, The Pirate Bay website had relocated to Iceland, after the Swedish authorities attempted to seize its domains, giving it an “.is” domain name. Within a week of the move, however, the site chose to relocate again outside of Iceland, even though ISNIC stated it had no intention of trying to seize the domain.25 According to Icelandic law, the registrant is responsible for ensuring that the use of the domain is within the limits of the law.26

Similar to other Nordic countries, ISPs in Iceland filter websites containing child pornography. The ISPs collaborate with the Icelandic Save the Children (called Barnaheill) and participate in the International Association of Internet Hotlines (INHOPE) project.27 In addition, pornography in general is illegal in Iceland, although the ban is not strongly enforced, and online pornography is not blocked.

In 2013, the previous minister of the interior, Ógmundur Jónasson, proposed two new bills in an effort to uphold and reinvigorate an existing law banning pornography and gambling online that is vaguely worded and rarely enforced. The ban focused on making it illegal to pay for pornographic materials with Icelandic credit cards, in addition to creating a national Internet filter and a blacklist of websites that contain pornographic content.28 Opponents led by Icelandic Member of Parliament and free speech activist Birgitta Jónsdóttir deemed that the ban would limit free speech online, a position that was supported by academics and free speech advocates from outside Iceland in an open letter to the Icelandic minister of the interior.29 The plan for banning pornographic content online has been stalled since the change in government during the parliamentary election on April 27, 2013. Since then, there have been no changes to the relevant legislation, and no changes have been formally proposed.30

Content Removal

In October 2014, the domain hosting company ISNIC, which operates the Icelandic .is domain, was

---

28 “Banning the Sex Industry - Naked Ambition,” The Economist, April 20, 2013, http://econ.st/12a1wwM.
30 Phone interview with an employee from the Icelandic Ministry of the Interior, May 12, 2015.
Iceland

forced to shut down a website for the first time when it discovered that the domain was being used by the self-described Islamic State terrorist group. The ISNIC’s board made the decision based on regulations holding the registrar responsible for ensuring that the use of the .is domain does not violate Icelandic laws.

Icelandic law number 30/2002 establishes a system of takedown notices for IP addresses or other online content that violates the law, in accordance with the Directive 2000/31/EC of the European Parliament. The Ministry of the Interior is responsible for handling matters related to online content, and the appeals process for disputing the removal of content goes through the independent courts in Iceland.

ISPs and content hosts are not held legally liable for the content that they host or transmit. Claims regarding intellectual property rights are handled by the Icelandic Patent Office, which is substantially dependent on international cooperation, and Iceland is party to a number of international agreements in this field. Moreover, as a member of the World Trade Organization (WTO), Iceland has adapted legislation to the provisions of TRIPS (Trade-Related Aspects of Intellectual Property Rights). Furthermore, the Agreement on the European Economic Area has led to several legislative amendments in Iceland that align with the directives and regulations of the European Union.

Media, Diversity, and Content Manipulation

Iceland has a vibrant digital sphere, and almost all traditional media, including print, radio, and television, offer versions of their content online. Self-censorship is not a widespread problem in Icelandic online media, and there are very few instances of government or partisan manipulation of online content.

The websites of some newspapers, like the daily Morgunbladid, are among the most popular Icelandic-language sites. Internet banking is widely used, and a large majority of Icelanders (93 percent) are online bank users. E-governance initiatives have been successful in Iceland and in recent years, public institutions have started a migration process from proprietary software to free and open software. The government promotes the use of digital signatures and electronic filing, and the use of digital signatures is supported through legislation such as the Public Administration Act. Digital signatures are in the process of being integrated further into the public administration.

Social media platforms such as YouTube, Facebook, Twitter, and international blog hosting services are freely available and are used by a large part of the population. In 2013 Iceland had the second highest number of Facebook users based on population percentage: 72 percent of the population has an account. Women make up 52 percent of users and men 48 percent, and the social networking site is mostly used by people aged 25-34, followed by people aged 18-24.

32 Gudmundsson, “Media Landscapes – Iceland.”
Iceland

Digital Activism

The popularity of social media sites like Facebook was used to engage the population in the process of redrafting the Icelandic constitution over the past few years. The original and existing constitution is an almost exact copy of the Danish constitutional text, which was adopted when Iceland gained independence from Denmark in 1944. In the wake of the Icelandic financial crisis in 2008, the population demanded an extensive review of the country’s constitution. A 25-member council consisting of ordinary residents helped draft a new constitution and worked through sixteen versions in four months based on 16,000 comments from Icelandic citizens using social media platforms such as Facebook, Twitter, and YouTube. A majority of the population voted for the draft constitution in a national referendum on October 20, 2012. In November 2013, the prime minister appointed a committee on constitutional affairs to continue the work on the constitution in accordance with an agreement reached by parliamentary parties. The committee issued a report in June 2014 concerning four priority political issues, and work on the next report was started after incorporating public comments and feedback and is to be issued in the fall of 2015. In accordance with current constitutional arrangements, the actual revision of the constitution will take place under the guidance of the parliament, with due consideration for the crowdsourced work done in recent years. Emphasis will be on transparency and informed debate, and the general public will participate. The aim is to present a bill before the next elections in 2017.

Although elections are not until 2017, according to a poll from March 2015, the Pirate Party, supporting online freedom and led by Birgitta Jónsdóttir, would become the largest in parliament with 29 percent of the votes, followed by the Independence Party with 23 percent if elections were held at the time of the poll. The Icelandic Pirate Party is aligned with a network of other similarly named political parties throughout the world that also promote a platform of free expression and has been the first Pirate Party to win seats in a national election (2013).

Violations of User Rights

Iceland has a strong tradition of protecting freedom of expression that extends to the use of the internet. The Icelandic Modern Media Initiative seeks to develop legal frameworks for protecting the press, bloggers, and whistleblowers from illegitimate prosecutions or harassment. Individuals are rarely prosecuted for social or political content posted online, though libel laws remain a concern. Government surveillance of online data is minimal, though reports over the past few years revealed that Icelanders’ data was subject to collection and monitoring by the NSA and its partners.

36 Robertson, “Voters in Iceland Back New Constitution, More Resource Control.”
39 Email interview with employee at the Legislative Department at the Office of the Prime Minister, April 27, 2013; and the website on the work with the draft constitution and constitutional matters in general: http://www.forsaetisraduneyti.is/stjornmarskra/.
41 Interview with employee at the Icelandic Media Commission, May 17, 2013.
Iceland

Legal Environment

Freedom of expression is protected under Article 73 of the Icelandic constitution. In June 2010, following the 2008 financial crisis and inspired by the whistleblower website WikiLeaks, the Icelandic parliament approved a resolution on the Icelandic Modern Media Initiative, which aims to create a global safe haven with legal protection for the press, bloggers, and whistleblowers. In 2012, the minister of education, science and culture appointed a committee of experts to report on online and offline challenges and propose recommendations for the promotion of freedom of expression and information. After a period with no incoming funds after the change in government in 2013, the new minister of education, science and culture recently assigned funding for the Icelandic Modern Media Initiative and appointed a new committee.

In March 2015, several bills concerning the safe haven objective of Iceland were submitted to Parliament, primarily by the Pirate Party as well as other members. The bills include whistleblower protection, a removal of a clause on data retention, and a resolution on establishing an office of Independent Oversight for police wiretapping procedures and other comparable investigative measures. As of May 2015, the bills have yet to be passed. In addition, a parliamentary resolution concerning the benefits of a free and unrestricted internet and the protection of user rights was adopted in late 2014 and awaits implementation in the near future.

The Icelandic Media Law, which came into effect in September 2011, established several legal protections for journalists that extend to the online sphere, including editorial independence from media service providers' owners and the protection of anonymous sources.

Prosecutions and Detentions for Online Activities

There has been great concern about libel laws in recent years with regard to both online and offline media. Journalists consider the court's practice with regard to libel laws to be too rigid, leading to lawsuits that aim to silence critical press. According to Article 51 of the Icelandic Media Law, journalists can no longer be held responsible for potentially libelous quotes from sources, but can only be held responsible for their own content.

In June 2014, civil servant Pòrey Vilhjálmssdóttir was falsely identified as the source in an information leak in the Ministry of the Interior, which led to the resignation of former Minister of Interior Hanna Birna Kristjansdóttir. The journalists corrected the statement without hours. Still, Vilhjálmsdóttir pressed defamation charges and sought the maximum punishment (two years in prison) as well as
Iceland

damages and legal costs against the journalists Jón Bjarki Magnússon and Jóhann Páll Jóhannsson, from the online and print newspaper DV, even though the journalists had publicly admitted their mistake. The case was closed when the newspaper DV settled against the will of the two journalists and payed ISK 330,000 (US$2,436) to Vilhjálmsdóttir.52

Surveillance, Privacy, and Anonymity

Following revelations that U.S. and UK intelligence agencies have been collecting and storing massive amounts of user data from online communications around the world, free speech activists in Iceland such as Birgitta Jónsdóttir expressed concern that Iceland’s efforts to protect journalists and whistleblowers from the threats of surveillance may ultimately prove ineffective.53 Iceland is part of a greater international surveillance network that cooperates with the activities of the “Five Eyes Alliance”—the intelligence operations agreement between the United States, the United Kingdom, Australia, Canada, and New Zealand.54

Currently, the Electronic Communications Act of 2003 implements data retention requirements mandated by Iceland’s inclusion in the European Economic Area.55 The law applies to telecommunication providers and mandates the retention of records of all connection data for six months. It also states that companies may only deliver information on telecommunications in criminal cases or on matters of public safety, and that such information may not be given to anyone other than the police or the public prosecution.56 The government does not place any restrictions on anonymous communication. No registration is required when purchasing a SIM card in Iceland.

Intimidation and Violence

There have been no physical attacks against bloggers or online journalists in Iceland.

Technical Attacks

In March 2015, the website of the Icelandic museum Njál’s Saga Center was hacked in the name of the terrorist organization Islamic State (ISIS).57 This followed an incident in October 2014, when ISNIC shut down a website that appeared to be run by ISIS.58

In December 2013, Iceland experienced its most serious cyberattack to date, when a Turkish computer hacker cracked Vodafone’s website.59 Since June 2013, the Icelandic National CERT, operating within the Post and Telecom Administration in Iceland, has been the national center point for cybersecurity incidents and participates in international efforts and cooperation.60

58 Eygló Svala Arnarsdóttir, “IS Terrorist Organization Picks Icelandic Domain.”
Key Developments: June 2014 – May 2015

- The Supreme Court struck down Section 66A of the IT Act in 2015, which had been the cause of several arrests for online speech, particularly on social media (see Legal Environment).

- Though the Supreme Court also upheld the IT Act’s Section 69A, which authorizes government blocking of online content, it did make the blocking process more transparent, and strengthened intermediary liability protection (see Blocking and Filtering and Content Removal).

- Website blocks ordered by the government or the courts temporarily affected entire platforms, such as Vimeo or Google Docs (see Blocking and Filtering).

- In April 2015, over 1 million people rallied to protect net neutrality and prevent regulation allowing telecommunications providers to charge extra for select services (see Digital Activism).
India

Introduction

The Bharatiya Janta Party (BJP) swept to electoral victory in 2014 under its leadership candidate Narendra Modi, and the new government completed its first year in May 2015. In the reporting period, India maintained its position as the third largest internet consumer base after the United States and China, and saw positive developments in terms of the regulatory framework, declining detentions for online speech, and burgeoning digital access. However, increased website blocking and intimidation of internet users threatened to hamper India’s steadily improving internet freedom.

A 2015 Supreme Court ruling dramatically impacted the regulatory framework governing the internet. The Supreme Court struck down Section 66A of the Information Technology Act 2000 (IT Act), which was amended in 2008, and which provides a legal framework for internet use. The Section had resulted in several arrests of individuals for political or social content published on social media between 2012 and early 2015. The Supreme Court also clarified intermediary liability protections for technology companies. Although it upheld Section 69A of the IT Act, authorizing government blocking of online content, it did make the blocking process more transparent through its interpretation of the law.

In the meantime, Indian law remains inadequate for the effective protection of privacy. Although a privacy bill is being drafted, reports indicate the law enforcement agencies are seeking to be exempt from the law, leaving its scope and effectiveness under question. There were no reported instances of unlawful surveillance in the present reporting period, although this may be due to the extreme opacity of the regulatory framework governing surveillance. News reports indicate that the government is continuing to develop the Central Monitoring System, its ambitious nationwide mass surveillance program directed at monitoring individuals’ digital communications.

Obstacles to Access

Internet penetration in India continued to increase in 2015, with mobile penetration once again playing a critical role in improving access. Infrastructure continues to remain a significant barrier; however, various governmental and nongovernmental initiatives such as the Digital India Initiative have been introduced in 2015 to address the inadequacies. Only one significant ICT shutdown was observed on account of a riot, but was lifted after three days. The top 10 internet service providers (ISPs) continue to hold almost the entire market share, but strong competition among them continues.

Availability and Ease of Access

With more than 302 million subscribers, India has the third largest number of internet subscri-
India

ers in the world after China and the United States. However, internet penetration remains low, reaching 24 percent in March 2015, up from 20 percent in June 2014.

Mobile penetration was much higher, reaching 77 percent by March 2015, with more than 969 million subscribers. Nearly 283 million of India’s total 302 million internet users were accessing the web through their mobile devices by March 2015. Wireless telephone access (through mobile) in India represents almost 98 percent of all telephone services, and accounts for nearly 94 percent of total internet access. India was ranked 113 out of 138 countries in terms of mobile broadband penetration by the Broadband Commission.

As of March 2015, there were nearly 16 million broadband subscribers, compared to just under 4 million narrowband subscribers, both excluding mobile access. Narrowband internet users declined from 76 percent of the total internet users, in March 2014, to about 67 percent by March 2015. Despite overall growth, India still has one of the world’s lowest high speed broadband (faster than 10 Mbps) adoption rate, at less than 2 percent.

The minimum speed required to qualify as broadband in India was raised to 512 kbps in 2012. However, this is one of the lowest average broadband speeds in Asia and remains below the global average speed of 5 Mbps. Akamai’s State of Internet report ranked India 115 out of 135 countries, measuring average speed at 2.3 Mbps.

The Global Information Technology Report 2015 ranked India first out of 143 countries for affordable internet access, with per minute cellular and fixed broadband tariffs among the lowest

4 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators January – March 2015, August 12, 2015, p. ii.
5 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators January – March 2015, August 12, 2015, p. i.
6 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators January – March 2015, August 12, 2015, p. i.
7 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators January – March 2015, August 12, 2015, p. i.
8 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators January – March 2015, August 12, 2015, p. i.
9 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators January – March 2015, August 12, 2015, p. ii.
11 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators January – March 2015, August 12, 2015, p. 28.
12 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators January – March 2015, August 12, 2015, p. 28.
India

in the world. However, inadequate infrastructure remains an obstacle to access. The Global Competitiveness Index 2014–15 ranked India 87 out of 147 countries for infrastructure, displaying a steady downward move from 85 out of 148 in the previous year. India ranked a low 103 for electricity supply, and 115 for technological readiness, the capacity of a country to fully leverage ICTs in daily activities.

In 2014, less than 20 percent of Indian schools had a computer; of those, less than a third were connected to the internet, and children were actually using them in only 7 percent of schools. Roughly 17 percent of villages in India have internet cafes. Kerala, historically an educationally advanced state, has internet cafes in 97 percent of villages. Yet, even in Kerala, more than half the households do not have a family member who knows how to operate a computer. Other geographically remote states such as Meghalaya, Arunachal Pradesh, Nagaland and Mizoram in India’s north-east, have internet cafes in less than 10 percent of villages, far below the national average. However, a 2013 industry-authored report indicated that Community Service Centres (CSCs) and Cyber Cafes provided internet access to 40 percent of the population. CSCs aim to bring e-services to every part of the country and thereby allow all citizens to access a variety of e-content. There has been a substantial 40 percent increase in their number since they were rolled out in May 2012. The government had established over 130,000 CSCs by 2014, with a goal of reaching 250,000 villages by 2017. In December 2014, news reports announced government plans to provide free public Wi-Fi zones, targeting 25 top cities by population. Some public Wi-Fi zones have already been established in places like Delhi, Ahmedabad, Bangalore and Patna.

The government launched the Digital India campaign in August 2014, co-ordinated by the Department of Telecom (DoT) and the Department of Electronics and Information Technology

29 Common Services Centres Scheme (CSC), Department of Electronics and Information Technology (DeitY), http://csc.gov.in.
India

(DeitY), and to be implemented by 2018.\textsuperscript{35} It aims to connect India’s Gram Panchayats, institutions of self-government for rural areas,\textsuperscript{36} via fibre-optic cables,\textsuperscript{37} ensuring universal broadband access with accompanying e-literacy programs. These infrastructure projects will also ameliorate the rural-urban divide. As part of its Digital India programme, the government has proposed to use satellites, balloons, or drones to push faster digital connections to remote parts of the country by March 2017.\textsuperscript{38} The government is planning to increase broadband penetration in smaller towns and rural areas through Multiple System Operators (MSOs), which include cable TV services, since such platforms already have last-mile connectivity in such areas.\textsuperscript{39}

Other non-governmental efforts at improving accessibility include Facebook’s Internet.org, in collaboration with Reliance Communications, to bring free access to a number of websites for subscribers,\textsuperscript{40} especially those who cannot afford data plans.\textsuperscript{41} However, the project came under extensive public criticism and several collaborators withdrew from the project (see Limits on Content).

Language continues to remain a barrier. Only about 12 percent of the population speaks English,\textsuperscript{42} yet more than half the content available is in English, according to one study,\textsuperscript{43} and more than 100 languages remain unrepresented online.\textsuperscript{44} At the same time, the number of local language users is growing at 47 percent year-on-year rate, with nearly 127 million local language users on the internet by 2014.\textsuperscript{45} Unsurprisingly, 42 percent of India’s internet users prefer to access content in their local language.\textsuperscript{46} Google’s Indian language Internet Alliance seeks to link all local language content available to a single platform,\textsuperscript{47} making it easier for consumers to navigate and making the content more visible.\textsuperscript{48} Critics fear this will divert traffic away from the

\begin{footnotesize}
\bibitem{35}
\bibitem{36}
Constitution of India, Article 243(d).
\bibitem{37}
\bibitem{38}
\bibitem{39}
\bibitem{40}
About, Internet.org by Facebook, http://www.internet.org/about.
\bibitem{41}
\bibitem{42}
\bibitem{43}
Usage of Content Languages for Websites, W3Techs, http://w3techs.com/technologies/httpw3techs.com/technologies/overview/content_language/all.
\bibitem{44}
\bibitem{45}
\bibitem{46}
\bibitem{47}
\bibitem{48}
India

original pages, resulting in loss of revenue and readership.\(^{49}\) Locally, the IAMAI has sought government incentives to boost local language content development.\(^{50}\) On December 25, 2014, the National Internet Exchange of India (NIXI), which operates and manages Indian domain names, launched the Dot Bharat domain under which URLs will now be available in local languages.\(^{51}\)

Studies have shown that economic and social conditions result in barriers to internet access for women. While there are almost 37 million active male internet users in India, there are only 21 million active female users.\(^{52}\) According to a study conducted by Google, women form only a third of India’s online population and almost half the country’s women do not see any benefit to access.\(^{53}\)

Restrictions on Connectivity

The Indian government does not routinely block the protocols or tools that allow for instant, person-to-person communication, though it sometimes limits ICT connectivity and usage during times of unrest. In September 2014 in Vadodara, an image widely circulated on Facebook was considered offensive to Islam by a number of Muslims, and as a result, led to clashes between Hindus and Muslims. When two persons were stabbed, the city police ordered mobile service providers to block 2G, 3G, SMS and MMS services for 3 days. Although wireline Internet access was not affected,\(^{54}\) pre-paid mobile SIM card sales were also temporarily halted.\(^{55}\) Service was restored after three days.\(^{56}\)

Submarine cables connect India to the global internet. Ten are consortium owned; the rest are private.\(^{57}\) These undersea cables are mainstays of mobile and internet communications and any damage to them leads to service disruptions. In February 2015, when two such cables – TGN and IMEWE

---


\(^{52}\) IMRB-INT, IAMAI Internet in India 2014, October 2014, p. 8.


\(^{57}\) The ten are: SeameWe-3; SeaMeWe-4; SeaMeWe-5; Asia-Africa Europe-1; Bay of Bengal Gateway; SAFE; Bharat Lanka Cable System; SEACOM/Tata TGN-Eurasia; IMEWE; and Europe India Gateway. See Submarine Cable Map, TeleGeography. [http://www.submarinecablemap.com/#/country/india](http://www.submarinecablemap.com/#/country/india).
India

—experienced faults, users reported being unable to access overseas platforms such as Twitter or Hotmail accounts via mobile, but the services were fully restored in the following two weeks.58

There are 10 cable landing stations in India – four in Mumbai, three in Chennai, and one each in Digha, Kochi and Tuticorin.59 While BSNL, the government-owned telecom operator, owns two of these stations, the rest are all privately owned. Tata Communications, which is the world’s largest owner and operator of fiber network,60 and Bharti Airtel, both of which are also major telecom operators, own three stations each.61 These cable-landing stations, where submarine cables meet the mainland, often impose hefty fees on ISPs; however, lower charges came into effect in 2013.62

Over 80 percent of telecommunications towers are privately owned.63 Market share was split between Indus Towers, a joint venture between Bharti Airtel, Vodafone, and Idea Cellular (32 percent); BSNL (15 percent); and Reliance Infratel (15 percent), according to 2011 figures.64 Bharti Infratel, a subsidiary of Bharti, is one of the largest tower infrastructure providers.65

ICT Market

There are 129 operational ISPs in India.66 While there is no monopoly, the top 10 ISPs control almost 98 percent of the market.67 Bharti holds the highest market share, worth 25 percent, followed by Vodafone (21 percent). BSNL, Idea and Reliance have around 10 percent market share each. There are 13 mobile operators, with Bharti controlling 23 percent of the market,68 followed closely by Vodafone (19 percent), Idea (16 percent) and Reliance (11 percent).69

The universal license framework, for which guidelines were published in November 2014,70 reduced the legal and regulatory obstacles for companies by combining mobile phone and ISP licenses, instead of requiring separate licenses for each sector. Licensees must now pay high one-

India

In 2011, the Indian government introduced rules under Section 79 of the IT Act requiring cybercafes to obtain a government-issued ID number in addition to a license, as well as to register and monitor customers. Critics said the rules were “poorly framed,” but penalties for noncompliance are unclear, and enforcement has reportedly been patchy. (CSCs are exempt, and operate under separate guidelines.)

Regulatory Bodies

The principal institution in India for the ICT sector is the Ministry of Communications and Information Technology. It consists of two departments – the Department of Electronics and Information Technology (DeitY) and the Department of Telecommunications (DoT). DoT manages the overall development of the telecommunications sector, licenses internet and mobile service providers, and manages spectrum allocation; DeitY formulates policy relating to information technology, electronics, and the internet. Internet protocol (IP) addresses are regulated by the Indian Registry for Internet Names and Numbers (IRINN). Since 2005, the registry has functioned as an autonomous body within the not-for-profit National Internet Exchange of India.

The Telecom Regulatory Authority of India (TRAI), an independent regulator, was created in 1997 to regulate the telecom, broadcasting, and cable TV sectors. The Telecom Regulatory Authority of India Act mandates transparency in the exercise of its operations, which include monitoring li-
India

licensing terms, compliance, and service quality.82 Its reports are published online, usually preceded by a multi-stakeholder consultation.83 A 2000 amendment to the Act established a three-member Telecommunications Dispute Settlement and Appellate Tribunal chaired by a former senior judge.84 The TRAI, which criticized government departments in 2013, is perceived to be largely free of official influence.85 Yet appointment and salary decisions for members remain in the hands of the central government. Further, while the TRAI Act initially barred members who had previously held central or state government office, amendments in 2014 diluted that prohibition, allowing them to join the regulator two years after resigning that position, or earlier with permission from the central government. Members may undertake commercial employment, except with telecom service providers.86

TRAI opinions, however, are generally perceived as independent. During the coverage period, for instance, its pricing recommendations for the 2100 MHz band spectrum auctions were repeatedly rejected by the DoT.87

Limits on Content

Content blocking increased during the coverage period with various instances of overbroad blocking and copyright restrictions. The constitutionality of Section 69A of the IT Act was upheld before the Supreme Court of India, but additional safeguards were interpreted. The intermediary liability guidelines issued under the IT Act, creating a notice and takedown system, were limited to exclude requirements for companies to respond to takedowns in case of user complaints. There was a significant increase in digital mobilization, especially on the issue of net neutrality.

Blocking and Filtering

Blocking of websites takes place under Section 69A of the IT Act, and a 2009 secondary legislation called the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules (“Blocking Rules”). The Blocking Rules empower the central government to direct any agency or intermediary to block access to information when satisfied that it is “necessary or expedient so to do” in the interest of the “sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the
commission of any cognizable offence relating to above. Intermediaries failing to comply are punishable with fines and prison terms up to seven years.

The Blocking Rules apply to orders issued by government agencies, who must appoint a “nodal officer” to send in requests and demonstrate that they are necessary or expedient under Section 69A. Those requests are reviewed by a committee which includes senior representatives of the law, home affairs, and information ministries, and the nodal agency for cyber security, the Indian Computer Emergency Response Team (CERT-IN). The “designated officer,” who chairs the committee, issues approved orders to service providers; the committee must also notify the source or intermediary hosting the content, who may respond to defend it within 48 hours. In emergencies and upon written recommendations from the designated officer, the secretary of DEITY may issue blocking orders directly, but the content must be unblocked if the designated officer does not obtain the review committee’s approval within 48 hours.

Indian courts can order content blocks without government approval. The designated officer is required to implement the court order after submitting it to the secretary of DEITY. Court orders can be challenged in a higher court, but internet users are not consistently notified of their implementation. ISPs are not legally required to inform the public of blocks and the Blocking Rules mandate that executive blocking orders be kept confidential. A 2014 transparency report issued by Verizon stated that the Indian government required the company to block access to websites, but that it was precluded by law from identifying how many blocking requests were received.

The 2011 cybercafe rules stated that cybercafes “may” install commercial filtering software “to avoid access to the websites relating to pornography, obscenity, terrorism and other objectionable materials.” It is not clear how many complied.

In the landmark Shreya Singhal case decided by the Supreme Court during the coverage period, the petitioners challenged the constitutionality of Section 69A, citing opaque procedure among other issues. However, on March 24, 2015, in the judgment of Shreya Singhal v. Union of India, the Supreme Court upheld Section 69A and the Blocking Rules, saying safeguards within the section were adequate, narrowly constructed, and not in contravention of the provisions of the Constitution of India. At the same time, the court read the Blocking Rules to include both the right to be heard and the right to appeal, changing the way Section 69A has been interpreted. It is now clear that blocking orders must provide a written explanation, allowing them to be challenged by writ petition, and that reasonable efforts must be made to contact the originator of the content for a pre-decisional hear-

88 Section 69A(1), The Information Technology Act, 2008.
89 Section 69A(3), The Information Technology Act, 2008.
91 Members must be of the rank of joint secretary or above, see Rule 7, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
97 Rule 6(5), Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
98 Common Cause v. Union of India [W.P(C) No. 21 of 2013]; PUCL v. Union of India [W.P(Crl) No. 199 of 2013]
100 [W.P. (Crl)No.167 of 2012]
India

ing before the blocking order is issued. However, given that the Blocking Rules require strict confidentiality to be maintained regarding the requests received, as well as the actions taken, it remains to be seen how and whether the judgment will be effectively implemented.

Implementation of blocks appears to depend on the technological capacity of ISPs. In 2013, Citizen Lab reported 90 instances of PacketShaper technology being used in India, 53 on public networks. PacketShaper can delay some or all packets carrying specific information, so that users seeking to access it experience unreliable service. On May 12, 2015, when the DoT ordered ISPs to block URLs advertising unlicensed taxi services like Uber, ISPs blocked two sites but said they lacked the ability to block others which were using HTTPS encryption. Separately in 2015, the state-owned BSNL stated that the Broadband Network (BBNW) Circle, established in 1988 to handle data services, has the capability to block entire websites only, not individual pages.

The number of blocked URLs increased during this reporting period, according to public information. Some of that information was contradictory. In a submission before the Supreme Court, the government said 2,455 URLs were blocked from January through December 6, 2014, of which 2,162 were blocked by court order and 293 through the committee constituted under Section 69A. Separately, in April 2015, the Minister for Communication and Information Technology told parliament that 2,091 URLs were blocked by court order in 2014 and another 143 between January 1, 2015 and March 31. A total of 255 URLs were blocked in 2014 under Section 69A through the committee, and none between January and March 31, 2015, according to the minister. While the reason for the different figures is unclear, however, the number of URLs affected is clearly rising. In 2014, the government said 1,299 URLs were blocked in compliance with court orders between January 2013 and January 31, 2014; and a further 62 URLs were blocked following the committee’s review. A single court order can block multiple URLs or domain names. For example, in reply to a Right to Informa-

104 “Some Devices Wander by Mistake: Planet Blue Coat Redux”, Available as part of data set for Morgan Marquis-Boire, Collin Anderson, JakubDalek, Sarah McKune, and John Scott-Railton, July 9, 2013. The data set may be accessed at https://docs.google.com/spreadsheet/pub?key=0AtJqKcMmUwTKdEMxMDk4VV80em1m1mc1RqVzFDeGNSVEE&output=html
110 Submission by the Union of India in the matter of PUCL v. Union of India W.P.(Crl) No. 199 of 2013. (On record with the authors).
In most cases, the content targeted through these orders is not known. However, there were multiple reports of overbroad blocks affecting legitimate online activity.

- On December 17, 2014, Deity blocked 32 websites based on a court order for “spreading anti-India messages by the ISIS terrorist group.” The blocks affected large platforms including Archives.org, Dailymotion, Vimeo, and Github, among others. Weebly, Vimeo, Github and Dailymotion were unblocked on December 31, but others remained blocked till January 9 2015. The government temporarily blocked the image sharing platform Imgur around the same time, but the reason remains unknown.

- In the aftermath of the attack on the satirical magazine Charlie Hebdo in Paris, the social media watch cell of the Mumbai Police intelligence went through potentially harmful posts on a popular social networking website and stated that they had blocked three to four posts carrying objectionable content. Although one newspaper said that over 650 pages or posts were blocked, the Mumbai police denied this.

- On June 23, 2014 the Delhi High court issued an order to block nearly 500 websites if they were found to be broadcasting the FIFA World Cup, whose exclusive broadcast rights were held by Multi Screen Media. The court revised the order in response to objections from the opposing counsels that the list was overbroad, including the URL for Google Docs.
the cloud-based document processing service. At least some users experienced disruption of listed services on some ISPs before the order was revised in July; it was withdrawn at the end of the event.

- In March 2015, the documentary *India’s Daughter*, directed by Leslee Udwin and produced by the BBC, was blocked online in India. The film tells the story of the 2012 rape victim, Jyoti Singh, whose case took India by storm in December of that year, inciting large-scale protests. On March 4, 2015, the government ordered blocking of its broadcast, filing a complaint with the Delhi Police, and obtaining a restraining order from the Delhi District Court against the screening in any form. A public interest litigation filed against the actions in the Delhi High Court remains pending. The video continued to be available despite the ban, as it was reposted multiple times.

The IT Act and the Indian Penal Code prohibit the production and transmission of "obscene material," but there is no specific law against viewing pornography in India, except child pornography, which is prohibited under the IT Act. In the case of Kamlesh Vaswani v. Union of India, a petition was filed asking the Supreme Court to direct the government to block all online pornography from view in India. In a 2013 order, the Supreme Court acknowledged this as an important matter, especially for children aged 14 to 18, and asked the government to "control the menace." In the past, the government has informed the Supreme Court that it is not technically feasible to block pornographic sites and that doing so will violate Articles 19 and 21 of the Constitution; however, the Supreme Court permitted the matter to be referred to the Cyber Regulation Advisory Committee.

---

123 CS(OS) 1860/2014 (July 1, 2014), High Court of Delhi (India) available at: [http://delhihighcourt.nic.in/dhcqrdisp_o.asp?pn=136945&yr=2014](http://delhihighcourt.nic.in/dhcqrdisp_o.asp?pn=136945&yr=2014)
130 Section 67(B), The Information Technology Act 2000.
committee consists of the telecom minister, government officials from DoT, DEITY, CBI and industry representatives.  

At a 2015 meeting of the Cyber Regulation Advisory Committee, the Minister of Communications and Information Technology asked the Internet and Mobile Association of India, an industry association, to monitor and prepare a list of pornographic sites for blocking by ISPs. A secretary for the Law Ministry said, “It is not desirable to submit the plea to Supreme Court that it is difficult to filter or block pornography sites and we must try to evolve a solution.”  

On August 31, 2015, outside the coverage period of this report, the government of India blocked access to 857 websites that are considered pornographic. DEITY asked DOT to notify the ISPs to implement the block, as these websites were found to be violating the morality and decency under Article 19(2). The order resulted in protests and backlash on social media and a widespread debate on censorship across India resulting in a subsequent order partially revoking the earlier order to limit the ban to only child pornography. Subsequently, the government informed the Supreme Court in the Kamlesh Vaswani matter that it would only block child pornography.  

Content Removal  

A 2008 IT Act amendment protected technology companies from legal liability for content posted to their platforms by others, with reasonable exceptions to prevent criminal acts or privacy violations. Intermediaries Guidelines issued in 2011 required intermediaries to remove access to certain content within 36 hours of a user complaint. The jurisprudence on notice and takedown changed significantly with the Supreme Court’s judgment in Shreya Singhal v. Union of India, in which the court read down Section 79 and the intermediary guidelines. While intermediaries had previously been required to take down content on receipt of user complaints, court orders, or government requests, they are no longer required to act on user complaints in the wake of the ruling. Further, the court order or government notification for removal of content will only be legitimate if it falls within the reasonable restrictions provided for under Articles 19(2) of the constitution, while earlier there was no requirement for the order to comply with Article 19(2). Unlawful content beyond the ambit of

---


136 Chinmayi Arun, “Blocking online porn: who should make Constitutional decisions about freedom of speech?” Scroll.in, February 3, 2015, http://archives.scroll.in/article/703746/blocking-online-porn-who-should-make-constitutional-decisions-about-freedom-of-speech


138 AdityaKalra, “India withdraws order to block pornography sites,” Reuters, August 5, 2015, http://in.reuters.com/article/2015/08/05/india-porn-ban-idINKCN0QA0KK20150805


140 Shreya Singhal v Union of India, Writ Petition (Criminal) No.167 Of 2012.
India

Article 19(2) cannot be restricted. Thus, the court restricted the earlier broad grounds for takedown notices.145

In February 2015, before the Shreya Singhal judgment, a comedic video titled “AIB Roast,” which was broadcast on YouTube, garnered more than 7 million views and prompted online and offline protests for content people called offensive. The organization apologized and removed the video from YouTube and other online video hosting platforms, though the content continued to be widely available.146 However, news reports said legal complaints were lodged against YouTube for distributing the content on grounds it was offensive.147 Separately, a petition filed before the Bombay High Court asking that YouTube videos be monitored for offensive content remains pending.148

The Indian government made 295 content removal requests to Google from January to June 2014, a marked increase from the 154 requests received between July to December 2013.149 Facebook received 4,960 requests for content removal from January to June 2014.150 Twitter received 15 requests for content removal from July to December 2014, of which 1 was court ordered and 14 were from police or government agencies.151

Intermediaries can separately be held liable for infringing the Copyright Act 1957,152 under the law and licensing agreements.153 The Shreya Singhal decision has had no impact on the legal framework on intermediary liability for copyright infringement. A 2012 amendment limited liability for intermediaries such as search engines that link to material copied illegally, but mandated that they disable public access for 21 days after receiving written notice from the copyright holder, pending a court order to remove the link.154 Rules clarifying the amendment in 2013 gave intermediaries such as search engines that link to material copied illegally, but mandated that they disable public access for 21 days after receiving written notice from the copyright holder, pending a court order to remove the link.154

---

152 In the Copyright Act, 1957, Section 51(a)(ii) read with Section 63 of Act criminalizes use of any place for profit for the communication of the work to the public where such communication constitutes an infringement of the copyright, exempting only those who are unaware or have no reasonable grounds for believing that such communication would constitute infringement of copyright. Moreover, Section 51(b) read with Section 63 also prohibits sale, hire, or distribution to the prejudice of the copyright owner, as well as exhibition in public and import to India of infringing copies also amount to infringement of copyright, with no exemptions. See, Pritika Rai Advani, “Intermediary Liability in India,” Economic & Political Weekly, December 14, 2013, Vol. XLVIII No. 50, p. 122.
153 The guidelines and license requirements for intermediaries also prohibit the carriage of copyright that infringes copyright or other intellectual property rights. Guideline 1.3(27), Guidelines and General Information for Grant of License for Operating Internet Services, http://www.dot.gov.in/data-services/internet-services; Unified License Agreement, Rule 38, http://www.dot.gov.in/sites/default/files/Amended.percent20UL.percent20Agreement_0.pdf.
India

aries power to assess the legitimacy of the notice from the copyright holder and refuse to comply. However, critics said the language was vague.

Media, Diversity, and Content Manipulation

Online media content is diverse and lively. In general, self-censorship is not widespread. Internet users in conflict regions may avoid addressing sensitive political or religious issues which other journalists and activists report freely. Some institutions and individual writers self-censor due to fear of reprisal from political organisations.

Social media users accused news outlets of removing controversial articles without explanation during the coverage period. An article by journalist Rana Ayyub about a prominent member of the ruling BJP party, published on the DNA news website on July 8, 2014, was taken down without explanation on July 12 after the critical piece prompted online discussion.

Economic forces also have the potential to influence online content. Paid news articles, or “advertorials,” are common in the mainstream media, ranging from unclear disclosure of paid endorsements to bribery and other kickbacks for coverage. In 2013, the Indian digital media website Medianama reported this phenomenon had increased on digital platforms in the past three years. Service providers took steps to limit access to communication tools which threatened their profits in 2014. In December 2014, Bharti Airtel planned to exclude Voice over Internet Protocol (VoIP) services from being accessed via regular data packages. The TRAI chairman told journalists this would not be illegal, as India lacked any laws protecting net neutrality, the principle that providers should not discriminate against certain content or data.

In February 2015, Facebook launched Internet.org in India, in collaboration with Reliance Commu-

---

India communications and other corporations. The service provides limited offline access to certain websites at no cost for Reliance customers without full internet access, reviving the net neutrality debate. On March 27, 2015, the TRAI issued a consultation paper envisaging a regulatory framework to support service providers charging extra fees for consumers using communication applications such as Viber, Skype, and WhatsApp, which the paper characterized as “over-the-top services,” going against the principles of net neutrality. The paper invited comments over a period of 29 days. This led to criticism and claims that the TRAI was hoping to minimize the public’s response by keeping such a short deadline. As a result of the criticism and the huge online mobilization, more than a million people submitted comments (see Digital Activism). Some corporations, including Clear Trip, NDTV and Times Internet, withdrew their content from Internet.org due to the negative publicity.

The DoT formed an eight-member panel to consider net neutrality in January; in May 2015, the panel had yet to release its report. The Parliamentary standing committee on Information Technology is also considering the issue of net neutrality.

Major political parties mobilized thousands of supporters using social networks in advance of the 2014 election. In November 2013, the Cobrapost news website exposed the practice of politicians paying around two dozen specialized IT companies nationwide to artificially boost their popularity and malign their opponents on social media. Their investigation particularly accused the BJP of this conduct.

The internet has given a voice to people in remote areas helping them become a part of the public discourse. The mobile news service CGNetSwara allows people in rural areas of central India to submit and listen to audio news reports, averaging 200 calls per day and driving the emergence of online reports on local issues that do not reach the mainstream media. The Delhi-based company Gram Vaani operates a Mobile Vaani initiative using an interactive voice response system to connect reports from mobile phone users to stakeholders including governments or NGOs. In Jharkhand and Bihar, it has over 400,000 users that call 5,000 times a day.

Digital Activism

Different instances of digital activism were observed in the reporting period. In December 2014, a

---

India

A different type of digital activism was seen in the “Kiss of Love” campaign, launched in October 2014 and spearheaded on Facebook, which mobilized people to protest against moral policing by ultra-conservative groups who object to public displays of affection. 179 Facebook blocked the Kiss of Love page following user complaints, but reinstated it the next day. 180 Support for the site grew, with many Facebook users posting pictures of themselves kissing. 181 The movement started in Kerala but collected supporters from cities all over India, including Kolkata, Bombay, 182 Hyderabad, 183 and Delhi, while events organized on Facebook saw significant turnout. 184

India

On February 6, 2015, women’s rights activist Sunitha Krishnan adopted a creative way of tracing alleged rapists with the “Shame the Rapist” campaign, which centered around a video demonstrating how to blur the face of victims in video footage of assaults shared on WhatsApp.185 The video went viral, garnering 16,000 views on YouTube,186 and an alleged rapist was arrested in March 2015 based on the shared images.187 Since then, Krishnan has received at least 90 videos submitted by rape survivors who had remained silent due to social stigma or fear. The Supreme Court has ordered an investigation into the alleged crimes portrayed in the footage188 and has asked the Government how to block dissemination of such videos.189

Violations of User Rights

Even though the number of criminal complaints regarding online content filed were quite high, arrests under Section 66A of the IT Act continued to decline in the reporting period. In a landmark judgment which will define the freedom of expression online in India, Section 66A was declared unconstitutional and all pending prosecutions dropped. However, charges under other sections continue to stand. Intimidation and violence against women was especially prevalent as a result of online activity. Online activity also led to an increase in religious tensions in two different incidents. The central authorities continue to develop the Central Monitoring System, which will allow officials to retrieve content and metadata from any electronic communication in India in real time.

Legal Environment

The Constitution of India grants citizens the fundamental right to freedom of speech and expression,190 including the right to gather information and exchange thoughts with others within and outside of India.191 Press freedom has been read into the freedom of speech and expression.192 These freedoms are subject to reasonable restrictions in the interests of state security, friendly relations with foreign states, public order, decency and morality, contempt of court, defamation, incitement to an offense, and the sovereignty and integrity of India. However, these restrictions may only be imposed by a duly enacted law and not by executive action.193 The right to privacy has been read into the right to life guaranteed by Article 21 of the constitution.194

The Indian Penal Code (IPC) criminalizes several kinds of speech, and applies to online content. Indi-

190 Article 19(1)(a), The Constitution of India.
individuals could be punished with a jail term ranging from two to seven years for speech that is found to be seditious, 195 obscene, 196 defamatory, 197 “promoting enmity between different groups on ground of religion, race, place of birth, residence, language,” 198 committing acts “prejudicial to maintenance of harmony,” 199 or consisting of statements, rumors, or reports that may cause fear, alarm, disturb public tranquility, or promote enmity or ill will. 200 Internet users are also subject to criminal punishment under the Official Secrets Act for wrongful communication of information that may have an adverse effect on the sovereignty and integrity of India. 201

The IT Act criminalizes certain online activity in particular. The act bans the publication or transmission of obscene or sexually explicit content in electronic form, and the creation, transmission or browsing of child pornography. 202

Through part of the reporting period, the IT Act included the infamous Section 66A, which criminalized information that was grossly offensive, of a menacing character, or any information which is false, but causes “annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will. This section led to several arrests for social media posts from 2012 through early 2015 before it was struck down by the Supreme Court on March 24, 2015 for violating Article 19 of the constitution. 203 The court affirmed that freedom of speech online is equal to freedom of speech offline, and held that Section 66A was an arbitrary and disproportionate invasion of the right to free speech outside the reasonable restrictions specified in Article 19(2). 204

**Prosecutions and Detentions for Online Activities**

A handful of prosecutions filed during the previous coverage period were still ongoing in 2014, while others were dropped for lack of evidence. 205 However, outstanding prosecutions under Section 66A will no longer be pursued in the wake of the Supreme Court’s March ruling, which declared it unconstitutional, though charges under other laws still stand. 206 Prior to that judgment, at least 10 complaints were filed and at least 4 arrests took place during the reporting period under Section 66A. The complaints and arrests were for different types of social and political content, much of it involving statements against politicians.

---

195 Section 124A, The Indian Penal Code, 1860.
196 Section 292 and 293, The Indian Penal Code, 1860.
197 Section 499, The Indian Penal Code, 1860.
198 Section 153A, The Indian Penal Code, 1860.
199 Section 153B, The Indian Penal Code, 1860.
200 Section 505, The Indian Penal Code, 1860.
201 Section 5, Official Secrets Act, 1923.
India

• In one November 2014 example, a case was registered against the Andhra Pradesh Chief Minister’s son for allegedly comparing K Chandrashekar Rao, the chief minister of Telangana, with Hitler.207

• In September 2014, a 25-year-old man was arrested under charges of sedition for booing the national anthem, and under Section 66A for allegedly publishing abusive social media posts about the Indian Independence Day. He was later denied bail. The charge was widely criticized.208

• In October 2014, a student was arrested in Andhra Pradesh under Section 66A and Section 153 of the IPC for a Facebook post celebrating a recent cyclone for “punishing” political opponents. He was released on bail.209

• In October 2014, police in the Malda district of West Bengal arrested a man accused of making a derogatory remark against Chief Minister Mamata Banerjee on her Facebook page. A court remanded him to 14 days’ judicial custody while his family sought bail.210

Surveillance, Privacy, and Anonymity

There is limited opportunity for anonymity on the internet in India. Pre- and post-paid mobile customers have their identification verified before connections are activated.211 There is a legal requirement to submit identification at cybercafes,212 and while subscribing to internet connections.

The effective implementation of privacy rights remains a significant issue. Communications surveillance may be conducted under the Telegraph Act,213 as well as the IT Act,214 to protect defense, national security, sovereignty, friendly relations with foreign states, public order, and to prevent incitement to a cognizable offense. Section 69 of the IT Act appears to add another broad category, allowing surveillance for “the investigation of any offence.”215

The home secretary at the central or state level issues interception orders based on procedural safeguards established by the Supreme Court and rules under the Telegraph Act.216 These are reviewed by a committee of government officials of a certain rank, and carried out by intermediaries.217

---


213 Section 5(2), Indian Telegraph Act, 1885.

214 Section 69, Information Technology Act, 2000.

215 Section 69, Information Technology (Amendment) Act, 2008.


217 Committee members are limited to a certain rank. JadineLannon, “Indian Telegraph Act, 1885, 419A Rules and IT
similar framework applies to the IT Act. Interception orders are not reviewed by a court and are limited to 60 days, renewable for a maximum of 180 days. Eight separate intelligence bodies are authorized to issue surveillance orders to service providers under these circumstances. Around 7,500-9,000 telephone interception orders are issued by the central government alone each month, according to a 2014 report citing information revealed in a right to information request.

Online intermediaries are required by law to “intercept, monitor, or decrypt” or otherwise provide user information to officials. Where the Telegraph Act levied civil penalties for non-compliance with an interception order while also creating the possibility of loss of license, the IT Act carries a possible seven year jail term. Unlawful interception is punishable by just three years’ imprisonment.

Some improvements to the framework have been made. On January 2, 2014, the government issued “Standard Operating Procedures (SOP) for Lawful Interception and Monitoring of Telecom Service Providers,” which were viewed by journalists but not publicly available. The procedures restricted interception to a service provider’s “chief nodal officer,” and mandated that interception orders be in writing. Rules issued in 2011 under the IT Act increased protection of personal data handled by companies. However, they do not apply to the government; critics say they create a burden on multinational companies, particularly in the context of the outsourcing industry.

These improvements failed to address the framework’s inconsistencies. In 2012, a government-appointed group of experts said the Telegraph and the IT Acts are inconsistent with regard to “permitted grounds,” “type of interception,” “granularity of information that can be intercepted,” the degree

---

221 Research and Analysis Wing, the Intelligence Bureau, the Directorate of Revenue Intelligence, the Enforcement Directorate, the Narcotics Control Bureau, the Central Bureau of Investigation, the National Technical Research Organization and the state police. See, Privacy International, “Chapter iii: Privacy Issues,” in India Telecommunications Privacy Report, October 22, 2012, https://www.privacyinternational.org/reports/india/iii-privacy-issues#footnoteref1_ni8ap74.
223 Section 69(4), Information Technology (Amendment) Act, 2008.
225 Information Technology Act, 2000, Section 69(4).
226 Indian Telegraph Act, 1883, Section 26.
of assistance from service providers, and the “destruction and retention” of intercepted material.” These differences, it concluded, “have created an unclear regulatory regime that is non-transparent, prone to misuse, and that does not provide remedy for aggrieved individuals.”

In early 2015, the Government was finalizing the draft of the Privacy Bill to be tabled in the Parliament. In August 2015, a three-judge bench of the Indian Supreme Court requested the Chief Justice to formulate a larger bench to decide whether privacy is a fundamental right in India.

License agreements require service providers to guarantee the designated security agency or licensor remote access to information for monitoring; ensure that their equipment contains necessary software and hardware for centralized interception and monitoring; and provide the geographical location, such as the nearest Base Transceiver Station, of any subscriber at a given point in time.

Under a 2011 Equipment Security Agreement that did not appear on the DoT website, telecom operators were separately told to develop the capacity to pinpoint any customer’s physical location within 50 meters. “Customers specified by security agencies” were prioritized for location monitoring, with “all customers, irrespective of whether they are the subject of legal intercept or not,” to be monitored by June 2014. The agreement remains effective, though various GSM operators lobbied for the clause to be removed from the license agreement because of compliance issues. In November 2014, an amendment to licensing conditions mandated government testing for all telecom equipment prior to use, effective in 2015.

Cybercafe owners are required to photograph their customers, arrange computer screens in plain view and software and hardware for centralized interception and monitoring; and provide the geographical location, such as the nearest Base Transceiver Station, of any subscriber at a given point in time.

236 Guideline 8, Guidelines and General Information for Grant of License for Operating internet Services, Department of Telecommunication, Ministry of Communication and Information Technology, Government of India, August 24, 2007.
239 In June 2014, outside the coverage period of this report, the DoT issued a letter to all Cellular Mobile Telephone Service Licensees, Unified Access Licensees and Unified Licensees, asking them to submit the status of implementation of location based services within seven days of receipt. Department of Telecom, Implementation of Location Based Services with Time Frame and Accuracy as Mandated by License Amendment dated 31.05.2011 to UASL – Reg. June 19, 2014, http://www.dot.gov.in/sites/default/files/DOC240614-005.pdf
India

sight, keep copies of client IDs and their browsing histories for one year, and forward this data to the government each month.\(^{240}\)

ISPs setting up cable landing stations are required to install infrastructure for surveillance and keyword scanning of all traffic passing through each gateway.\(^ {241}\) The ISP license bars internet providers from deploying bulk encryption; restricts the level of encryption for individuals, groups or organizations to a key length of 40 bits;\(^ {242}\) and mandates prior approval from the DoT or a designated officer to install encryption equipment.\(^ {243}\)

Since 2011, officials have sought to prevent international providers from encrypting user communications,\(^ {244}\) and required some, such as Nokia and BlackBerry, to establish local servers subject to Indian law under threat of blocking their services.\(^ {245}\) In 2013, BlackBerry confirmed their “lawful access capability” met “the standard required by the Government of India,” though business customers would be unaffected.\(^ {246}\)

The Indian government also seeks user information from international web-based platforms. According to the Google Transparency Report, the government made 3,112 user data requests and 4,684 requests to access accounts between July and December 2014,\(^ {247}\) the second highest number of requests from any single government.\(^ {248}\) The government requested access to 5,958 Facebook accounts between January and June 2014, and some data was produced in 51 percent of cases.\(^ {249}\) Twitter received 113 account information requests pertaining to 2,963 accounts from January to June 2015.\(^ {250}\) Yahoo received 1,001 government data requests involving 1,178 accounts from July to December 2014, showing a decline from the first half of 2014.\(^ {251}\)

Besides retrieving data from intermediaries, the government’s own surveillance equipment is becoming more sophisticated. The 2013 announcement of a Central Monitoring System (CMS), which will allow government agencies to intercept any online activities, including phone calls, text messages and VoIP communication directly using Lawful Intercept and Monitoring (LIM) systems on intermediary premises, caused widespread concern.\(^ {252}\) Execution of the CMS has been entrusted to

\(^{240}\) Rule 4, Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
\(^{241}\) Guideline 42, Guidelines and General Information for Grant of License for Operating internet Services, Department of Telecommunication, Ministry of Communication and Information and Technology, Government of India, August 24, 2007.
\(^{242}\) Guideline 13(d)(vii), Guidelines and General Information for grant of License for Operating internet Services, Department of Telecommunication, Ministry of Communication and Information and Technology, Government of India, August 24, 2007.
\(^{243}\) Guidelines and General Information for grant of License for Operating internet Services, Department of Telecommunication, Ministry of Communication and Information and Technology, Government of India, August 24, 2007.
India

the DoT’s Centre for Development of Telematics.253 New reports differed as to when it would become operational,254 but at least one cited significant technical shortcomings preventing the system from coming online in 2013.255 A minister told parliament in early 2014 that it is being phased in over the next three years,256 and in 2015 the parliament was informed that New Delhi and Karnataka have been chosen for the initial phase.257 In the meantime, licensing agreements were amended to require the licensee to provide connectivity up to the nearest point of presence of the CMS network at its own cost.258

In 2015, news reports said a lab under the Defence Research and Development Organisation (DRDO) was preparing to launch “NETRA,” short for Network Traffic Analysis, a system to sweep online content for keywords like “bomb.”259 The timing for its release is not known.

Intimidation and Violence

While there is no systematic violence against internet users, many are periodically targeted in reprisal for online activities, including during the coverage period of this report.

Women are particularly vulnerable. In July 2014, a social activist complained to the Bangalore police after a man posted a comment on her Facebook wall calling for women like her to be raped.260 In February 2015, activist Sunitha Krishnan, who started the “Shame the Rapist” campaign on social media, was subject to an attack where her car was stoned by some people smashing the rear window, just two hours after she posted the video.261

Social media also inflamed religious tensions. In June 2014, protests by a right wing Hindu mob in Pune, Maharashtra, against images posted on Facebook resulted in the killing of a Muslim man, though he was not associated with the content.262 Separately, in October 2014, an offensive image relating to Islam posted on Facebook sparked four days of violence in Vadodara, a city in Gujarat.263

---


India

As in many countries, digital technology also played a disturbing role in helping criminals promote violence against women. In February 2015, three men were arrested under Section 376 of the IPC (which criminalizes rape), the Protection of Children from Sexual Offences Act, and the IT Act, on suspicion of gang rape and distributing video and photos of the incident on WhatsApp and YouTube.²⁶⁴

Technical Attacks

In September 2014, Communications and IT Minister Ravi Shankar Prasad said a total of 96,383 security incidents including phishing, scanning, spam, malicious code, and website intrusions, were reported to the Indian Computer Emergency Response Team.²⁶⁵ Other reports said cybercrime had registered an annual increase of more than 40 percent in the past two years.²⁶⁶ Governments and corporations are the primary targets.

Many attacks are reported to have originated in Pakistan, including a November 2014 breach of 22 government department and organization websites of Andhra Pradesh, Telangana, and Odisha states.²⁶⁷ In December, the website of the Sri Meenakshi Sundareswarar Temple in Madurai was defaced by a hacking community called Pak Teen Leets through a U.S.-based server.²⁶⁸


Indonesia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>42</td>
<td>42</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 251 million
Internet Penetration 2014: 17 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2015 Status: Partly Free

Key Developments: June 2014 – May 2015

- The Supreme Court upheld a Ministerial Regulation on “negative content” passed without legislative review, which gives officials the power to block websites (see Blocking and Filtering).

- Video-sharing platform Vimeo was officially blocked in Indonesia for hosting allegedly pornographic content in May 2015, though implementation varied by ISP (see Blocking and Filtering).

- At least five people were sentenced to prison under the notorious Information and Electronic Transactions Law (ITE Law), which the government pledged to revise in 2015 (see Prosecutions and Detentions for Online Activities).
Indonesia

Introduction

Joko Widodo, former governor of Jakarta and mayor of Solo, was inaugurated as Indonesia’s seventh president on October 20, 2014, ushering in a new administration. The legislative election in May 2014 was followed by the presidential election in July, but the transition was delayed by a failed challenge mounted in the Constitutional Court by the losing candidate.1

The third direct presidential election since the democratic transition in 1998 was highly polarizing. Indonesia, the world’s third largest democracy, mobilized 187 million voters, including 67 million voting for the first time, and the close result lead to heated debates on social media.2 Online campaigning was increasingly influential.3

The 1998 transition paved the way for stronger protection of human rights, including freedom of expression, through constitutional and legal reform. Vibrant civil society organizations continue to play a major role in democratization, and economic development has increased the middle class population.4 Internet access continues to expand, though infrastructural challenges remain, while affordable smartphones have helped embed digital communication in daily life.

With an estimated 64 million Facebook accounts, 20 million Twitter users, and 5 million active bloggers, the internet is transforming the social and political landscape in Indonesia.5 Mobile devices are the medium of choice for the majority of Indonesians who wish to access the internet.6 Awareness of the internet’s potential to facilitate mobilization around social causes has been widely recognized. However, religious intolerance is also on the rise, and the internet has been exploited to spread hate speech.7

Digital expression also comes with possible criminal sanctions, especially for defamation, which is more heavily penalized online under the Information and Electronic Transactions Law (ITE Law) than it is under the penal code. The number of charges filed under the defamation clause increased from 10 in 2012 to 41 in 2014. The new minister of ICT pledged to revise the problematic ITE Law by the end of 2015, but the promised reform still fell far short of international standards.8

On July 17, 2014, the outgoing Ministry of Communication and Information enacted a regulation granting ministry officials broad powers to filter “negative” content on the internet.9 After blocking

---


413 www.freedomhouse.org
Indonesia

several websites, the new ICT Minister faced heavy criticism from the media and civil society groups, and created four panels made up of civil society representatives and governments officials to assess the content reported for blocking—though the process still lacks judicial oversight.10

Obstacles to Access

While smartphone use is increasing, the total internet penetration in Indonesia remained under 30 percent of the population. This low access rate is mainly due to the geographic conditions of Indonesia, which consists of 17,000 islands and a population that is concentrated in the major islands, namely Java and Sumatera.

Availability and Ease of Access

Internet penetration continued to increase over the past year, though precise figures differed. The International Telecommunication Union cited 17.14 percent in 2014, up from 14.94 percent in 2013.11 Indonesia’s ICT Ministry reported 73 million internet users in Indonesia, which would put penetration at almost 30 percent.12

Mobile penetration was 127 percent in 2014,13 while smartphone penetration was at 21 percent in 2014 and projected to increase to 26 percent in 2015.14 Mobile phones have become the preferred method to access the internet for most Indonesians, overtaking computers.15 Internet users spend an average of five hours a day online.16

Affordable devices are available, and phones with Android operating systems start at US$30. Multiple SIM cards and devices are common, as people shop around for better signal quality and lower connection prices.17 Prepaid internet packages for smartphones range from US$0.50 a day to $2.50 a month. As mobile phones became more popular, the number of fixed-line internet subscribers has decreased. In urban areas, most shops and cafes provide free Wi-Fi, as do public libraries and schools.

Competition among internet service providers (ISPs) has reduced the cost of connection and made internet use more accessible. In the past, access was concentrated among older urban residents. In 2013, however, 70 percent of Indonesia’s online population was under the age of 35.18

Restrictions on Connectivity

Internet access continues to be concentrated in major cities such as Jakarta and Sumatera due to poor infrastructure in rural areas, particularly in the eastern part of the archipelago.\(^\text{19}\) By 2012, there were 41 fiber-optic backbone cables, of which 60 percent were located in Java. Less than 2 percent reached Bali and the group of nearby Nusa Tenggara islands.\(^\text{20}\) In 2013, a Moluccan Ring cable system was launched to connect Papua and other parts of eastern Indonesia with the existing broadband network.\(^\text{21}\)

This gap is even wider for high-speed 3G internet access, as most base transceiver stations (BTS) which facilitate the connections are built by private providers, who determine the number and location based on the market. The highest concentration is in West Java, where there are nearly 10,000 stations, followed by Jakarta with 6,800. There are less than 1,000 3G BTS in Papua, Kalimantan, and the Mollucan Islands combined.\(^\text{22}\) In Papua, less than 40 percent of the population owned a mobile phone in 2013, compared to 97 percent in Jakarta.\(^\text{23}\) A national 2012 survey put e-literacy in underdeveloped provinces such as Papua and Mollucan far lower than the national average.\(^\text{24}\)

The Ministry of Communication and Information (MCI) has made infrastructure a priority since 2010, developing subdistrict internet service provider (PLIK) and subdistrict internet service vehicle (MPLIK) programs to improve connections in the subdistricts that make up the regencies and cities in Indonesian provinces. Other programs, such as desa berdering (ringing villages), and desa pintar (smart villages), target villages without private internet providers.\(^\text{25}\) A 2012 ICT white paper set out to eliminate the digital divide by connecting 33,000 villages.\(^\text{26}\)

In 2013, the Attorney General’s Office opened a criminal investigation naming government officials and private sector businessmen as suspects in alleged corruption involving an infrastructure budget of US$100 million. The investigation was ongoing at the end of the coverage period of this report.\(^\text{27}\) The development project has been suspended citing inefficiency, pending further evaluation.\(^\text{28}\)

ICT Market

There are about 300 ISPs operating in Indonesia. However, 10 major providers dominate the market, and 3 retain the biggest market shares. Two of them are partly state-owned enterprises: PT Telkom-
Indonesia

 sel, with a market share of 60 percent, and PT Indosat with 21 percent. A third, XL-Axiata, accounted for 19 percent. In December 2014, Telkomsel launched 4G-LTE services in the Jakarta and Bali areas, offering faster service that was soon matched by XL-Axiata and Indosat.

In 2013, the Attorney General’s Office filed corruption charges against one ISP, IM2, for selling bandwidth under a public frequency licensed only to its parent company, Indosat. IM2 was accused of avoiding a private tax rate on the frequency, causing state losses of IDR 1.3 trillion (US$134 million). Since ISPs generally rent frequencies from other companies in Indonesia, the APJII condemned the investigation. The MCI agreed the practice was in line with ministerial regulations, and practiced by about 280 other ISPs. However, the same year a court sentenced IM2 CEO Indar Atmanto to four years in prison and ordered Indosat to pay IDR 1.3 trillion in compensation. An appeal court rejected the defendant’s appeal and increased the CEO’s sentence to eight years imprisonment, although it removed the fine. Both Indosat and the attorney general appealed to the Supreme Court. In July 2014 the Court upheld the initial verdict, the eight year prison term for Indar, and reinstated the fine. Indar filed a judicial review to the Supreme Court again in March 2015. No ruling had been announced at the end of the coverage period.

The consequences of this ruling will affect almost all Indonesian ISPs, since so many are renting public frequency from telecommunication companies that have been awarded the rights to use the frequency by paying the Indonesian government. In September 2014, Onno W. Purbo, a well-known ICT figure in Indonesia, started a petition on Change.org in support of Indar Atmanto.

Regulatory Bodies

The Directorate General Post and Telecommunication Resources and Directorate General Post and Informatics oversee internet services under the MCI. Their mandates include regulating the allocation of frequencies for telecoms and data communications, satellite orbits, ISP licenses, and overseeing private telecom providers. In January 2014, the Internet Defender Front (FPI) and APJII filed a constitutional review of the Law on Post and Telecommunication due to the high cost it prescribes for an ISP license. In March 2015, the Indonesian Constitutional Court rejected the claim and found the existing law constitutional. However, the APJII continues its campaign to get the law revised, including calls for parliament to review it.

---

32 Conversion as of January 15, 2013, according to Oanda. The value of the rupiah plunged in 2013; as of July 19, 2013, when news reports announced the verdict, the same amount came to US$128 million.
37 Twelve ISPs were closed down by the government in 2012 after failing to produce the fee. See, “FPI dan APII Gugat Biaya Tinggi Usaha Telekomunikasi,” Jurnal Parlemen, January 17, 2014, http://bit.ly/1nYlsSW.
Indonesia

In 2003, a more independent regulator, the Indonesia Telecommunication Regulatory Body (BRTI), was established to oversee fair competition among telecommunications business entities, to resolve industry conflicts, and to develop standards for service quality. The appointment of the head of the MCI’s Directorate General Post and Telecommunication as chair raised concerns over its independence, though its composition has been balanced. In May 2015, new BRTI members for 2015-2018 were announced, including three government officials and the remaining six from civil society. Despite this, the body lacks executive power, and can only make recommendations. As a result, it fails to intervene in relevant fraud or corruption cases, and its effectiveness remains challenged.

Limits on Content

The MCI regulation on “negative content” was authorized during the coverage period, officially giving power to the MCI to block content deemed pornographic or illegal. This was followed by the creation of four panels to act as consultation councils for different banned topics such as child pornography, hate speech, fraud, fake drugs, illegal investments, gambling, and intellectual property rights. These events were continually challenged by civil society groups, which identified a threat to freedom of expression in the new censorship powers issued without a legislative process.

Blocking and Filtering

The authority to block content is granted by the Information and Electronic Transactions Law (ITE Law), provided that limitations are in the public interest and intended to maintain public order. In practice, blocking tends to be arbitrary, as the wording lacks clarity in its articulation of what is considered as “forms of disturbance,” “abuse of electronic information,” “public interest,” and “public order.” Another statute provides a legal framework to block content considered pornographic.

In practice, the MCI has long played a role in managing what content is blocked, but that role was formalized during the coverage period. As one of his last acts in office, former ICT minister Tifatul Sembiring authorized Minister Regulation no. 19/2014 on “negative content” in July 2014 before his position was replaced in the new cabinet. The objective of the regulation was to provide a legal procedure for the government to restrict “negative” websites, with “negative” defined as containing pornographic or otherwise illegal material, under existing Indonesian law.

The regulation specified the existing service Trust Positive as the government’s “blocking service provider,” or database of websites with negative content for Indonesian ISPs to block.


44 See, Law No. 11/2008, Article 40.

45 Civil society and cultural groups challenged the law before the Constitutional Court in 2009 for its narrow and obscure definition of pornography and pornographic content, which includes LGBTI content and folk traditions which expose the female form, such as the Jaipongan folk dance from West Java and Papuan traditional clothes. The Court upheld the Law.

Indonesia

is a filtering application operational since 2010, managed directly by the ministerial office, with a database of continuously updated websites. In 2015, the Trust Positive website listed 763,126 websites blocked. The majority of blocks come under the category of pornography. Other categories include radicalism, hate speech, fraud, gambling, child violence & pornography, internet security, intellectual property rights, violence and miscellaneous.

The regulation also detailed procedures for the public to report negative content online or via email, and how to appeal in case of wrongful blocking. Members of the public or website owners can file complaints to remove the website’s URL address from the Trust Positive database of banned sites, and the complaint must be resolved in 24 hours.

ISPs are obliged to implement ongoing blocks based on the database, which functions as a minimum list of required blocks, so each ISP can add more sites. As each ISP can employ different software for blocking, and create independent databases, content restrictions are inconsistent. In the past, researchers were unable to identify whether blocks implemented by three ISPs were based on Trust Positive or an independent list. This creates uncertainty for users seeking redress when content is wrongly blocked.

In November 2014, the regulation was subject to a Supreme Court judicial review after a challenge was filed by several NGOs and individuals. The challenge said there was no clear law by which MCI officials could assess content, and that the regulation represented a threat to citizens’ constitutionally guaranteed freedom of expression. In May 2015, the Indonesian Supreme Court rejected the application.

With the new ICT minister Rudiantara in office, requests to block websites under the regulation began to appear in October 2014. Some of the blocks appeared to target criminal activity. By December 2014, the ICT Ministry reported that they have blocked 400 websites for selling fake drugs, and another 45 websites offering unregistered marriage services. Other examples were less clear, like a YouTube video showing bullying in an elementary school in Bukittinggi, Padang, which was blocked at the request of an individual. The blocking of 19 websites for allegedly radical Islamic teaching also attracted public criticism.

In response to these objections, Rudiantara announced the creation of four panels to review each website reported for blocking. The four panels cover pornography and child abuse; terrorism, hate speech; illegal investment, fraud, gambling, food and drugs; and copyright infringement. Responding to the panels, the Institute for Criminal Justice Reform stated that any effort to limit citizens’ rights must undergo legislative review, and that doing so by ministerial regulation violates the constitution.

47 Trust Positif, website, http://trustpositif.kominfo.go.id/.
Indonesia

The video service provider Vimeo became inaccessible on many ISPs in mid-2014, apparently in response to an MCI directive to individual ISPs and the site’s inclusion in the Trust Positive database for allegedly pornographic content. (Vimeo bars sexually explicit content in its terms of service.) Though implementation of the directive remained intermittent, blocking was documented by users and by researchers at the University of Toronto-based Citizen Lab. In November 2014, the ICT minister asked internet users to participate in a dialogue with Vimeo’s CEO after the company declined to modify its terms of service for the Indonesian market. Despite dialogue during the coverage period, which included civil society representatives, Vimeo and the ICT Ministry still cannot agree on a way to filter allegedly pornographic material selectively for Indonesian users. As a result, Vimeo remains officially blocked from use in Indonesia.

Since filtering relies on keywords, blocks can be overly broad. Some minority voices, particularly LGBTI groups, suffer from arbitrary filtering. In April 2013, the LGBTI group website Our Voice could not be accessed on the XL-Axiata network, though it was available through other providers, such as Telkomsel and First Media. After investigating the group’s complaint, the provider was unable to determine if the group’s domain fee had lapsed, or if it was formally blocked. In June, XL-Axiata’s customer service said on its company Twitter account that Our Voice was listed in the Trust Positive database, which the MCI denied. However, after the APJII intervened, the blocking was ultimately lifted in September. It apparently stemmed from the inclusion of keywords such as “gay” and “lesbian” in the database.

Besides the MCI, the independent Nawala Foundation provides a free DNS server enabling service providers to block hundreds of thousands of websites for content including pornography and gambling. Its database included 811,190 sites by January 2014, but no longer issued statistics in 2015.

Content Removal

Administrative requests to delete or take down content are less common. From January to June 2014, Google reported two government requests to remove content from its platforms, involving defamation and nudity. The government has threatened service providers for failing to implement censorship in the past. In 2011, BlackBerry agreed to filter pornographic websites on their devices in

---

Indonesia

Indonesia after the government regulator warned that the firm’s market access could be restricted if it failed to comply.65

Media, Diversity, and Content Manipulation

Journalists and internet users did not exercise undue levels of self-censorship during the coverage period of this report. Interference from state agencies has declined significantly compared to past years, but social pressure still periodically leads to self-censorship among journalists, and occasionally manifests online in relation to religion, sensitive political corruption charges, or potential defamation.66

Indonesia has enjoyed a thriving blogosphere since around 1999, though traditional media outlets—rather than blogs—typically cover important political developments and corruption investigations. Indonesians are also avid users of social media and communication apps, which are freely available. However, social media growth has produced new concerns about content manipulation. Analysts say anonymous or pseudonymous Twitter accounts circulating politically motivated rumours and attacks on politicians may be part of sponsored campaigns to influence online discourse, or even blackmail well-known figures seeking to protect their reputations.67 Social media pages have also been used by religious extremists.68

Digital Activism

The internet has also strengthened grassroots mobilization. The Indonesia Breastfeeding Mothers Association (@aimi_as) has embraced social media, circulating kultwit, or short Twitter lectures, on breastfeeding for new mothers and other reproductive health issues to reach women across the country. In more urban settings, community movements have used social media to maintain the spirit of volunteerism. The @idberkebun network, which promotes urban farming and conservation, has spread to 30 cities and 8 universities in four years,69 using digital forums to provide free classes and organize community farming on abandoned land. Similarly, the @akademiberbagi network facilitates learning and sharing between people and experts on different topics.70

During the election year, digital activism was focused more on political campaigning from many sides and parties. Two were particularly notable. One used the hashtag #ShameOnYouSBY, initials which refer to former President Susilo Bambang Yudhoyono, when his Democratic Party withdrew support for direct elections for regional heads, a move which critics said undermined the democratic process that Indonesian has enjoyed so far.71 The second campaign was the ongoing #SaveKPK

---

69 See, Indonesia Berkebun, “About,” http://indonesiaberkebun.org/about/
Indonesia

and #AkuKPK movement in support of Indonesia's Corruption Eradication Committee, known by its abbreviation KPK. The committee came under political attack after successfully documenting politicians and judges caught receiving bribes, but the public display of support prevented it from being disbanded.72

Violations of User Rights

The number of people prosecuted under the ITE Law has increased, often to intimidate and to silence critics. People frequently use the law for their own agenda, misguidedly mixing public and private digital space. Hope lies with the new ICT minister's promise to revise the ITE Law by the end of 2015. However, without proper training offered to Indonesian law enforcement and judiciary, more erroneous prosecutions are likely to occur.

Legal Environment

Freedom of expression was initially protected through the stipulation of the Law on Human Rights, shortly after the 1998 reformation, which was strengthened through the second amendment of the constitution in 2000. The third amendment guarantees freedom of opinion.73 The constitution also includes the right to privacy and the right to obtain information and communicate freely.74 These rights are further protected by various laws and regulations.75 Indonesia also ratified the International Covenant on Civil and Political Rights (ICCPR) in 2005.76

Other laws passed since then have infringed on user rights, despite legal experts' opinions that they conflict with the constitution.77 The antipornography law introduced in 2008 contains a definition of pornography which can be loosely interpreted to ban art and cultural expression perceived as explicit.78 A 2011 State Intelligence Law introduced penalties of up to ten years' imprisonment and fines of over US$10,000 for revealing or disseminating “state secrets,” a term which is vaguely defined in the legislation.79 This framework provides authorities with a range of powers to penalize internet users, even though not all are regularly implemented. Some civil society groups challenged this law in the Constitutional Court, which rejected their petition in 2012.80

Provisions of the 2008 ITE Law have been used repeatedly to prosecute Indonesians for online ex-

73 Constitution of 1945, Article 28E(3).
74 Constitution of 1945, Articles 28F and 28G(1).
76 The ICCPR was ratified through Law No. 12/2005. However, to date the government has yet to review and reform laws to comply with the covenant's human rights standards.
Indonesia

pression. The law’s penalties for criminal defamation, hate speech, and inciting violence online are harsh compared to those established by the penal code for similar offline offenses. Sentences allowed under Article 45 can extend to six years in prison; the maximum under the penal code is four years, and then only in specific circumstances—most sentences are less than a year and a half.81 Financial penalties show an even more surprising discrepancy. While the ITE law allows for fines of up to IDR one billion (US$80,000), the equivalent amounts in the penal code have apparently not been adjusted for inflation. Article 310, for example, allows for paltry fines of IDR 4,500 (US$0.37) for both written and spoken libel.82

The MCI promised to revise the ITE Law by the end of 2015. However, the focus of this revision would reportedly be a single article on online defamation, reducing the maximum prison sentence from six to four years in prison. This would move the offense from the category of serious crime to regular crime, but would not decriminalize the offense or check the abuse of the law to suppress free speech.83

Prosecutions and Detentions for Online Activities

By March 2015, the number of individuals sued under the ITE Law since 2008 had increased to 85.84 At the end of 2014, that figure was 74, with 92 percent of cases filed for online defamation, 5 percent for blasphemy, and 1 percent for online threats. The number of prosecutions under the ITE Law almost doubled in 2014, with a total of 41 cases, up from 21 in 2013.85 Recognizing the problematic elements of the law and the number of misguided charges filed, the new administration promised to revise the law by the end of 2015.86

Problematic sentences were also passed during the coverage period:

- In February 2014, Fadli Rahim, a government official in Gowa, South Sulawesi Province, was sentenced to eight months in prison for defaming Gowa’s Regent, Ichsan Yasin Limpo, on LINE Messenger.87

- In March 2015, Florence Sihombing, a student in Yogyakarta, was sentenced to two months in prison for defaming the city of Yogyakarta in an August 2014 post on the social network Path. Observers took a screenshot of the message, which subsequently went viral, calling the city “stupid, poor and uncivilized.”88

- In March 2015, Agus Slemet and Udin, NGO activists in Tegal, Central Java Province, were

82 "Kitab Undang-Undang Hukum Pidana" [Criminal Law], available at Universitas Sam Ratulangi, http://bit.ly/1KZOGuY
Indonesia

sentenced to five months in prison after posting a modified photo of Tegal Mayor Siti Mashita on Facebook.89

- In March 2015, Wisny Yetty, a housewife in Bandung, West Java, was sentenced to five months in prison for an allegedly “immoral” private message sent to a Facebook contact accusing her ex-husband of domestic violence. The message was reported by the ex-husband, who accessed her account without permission.90

In January 2015, Ervani Handayani, a housewife in Yogyakarta, was acquitted of defamation charges filed in response to her posting a complaint about her husband’s supervisor on Facebook.91

Surveillance, Privacy, and Anonymity

Mobile phone users are technically required to register their numbers with the government by text message when they buy a phone, though this obligation has been widely ignored in practice. Some telecommunications companies are known to have complied with law enforcement agencies’ requests for data. In 2011, amid concerns that Blackberry’s encrypted communication network would hinder antiterrorism and anticorruption efforts, the company reportedly cooperated with the authorities in isolated incidents, and agreed to establish a local server, though in Singapore, not in Indonesia.92 The government introduced a regulation in 2012 requiring electronic system providers offering “public services” to build local data centers, and a draft regulation in 2014 laid out technical requirements for any entity offering “information technology-based services” to comply, but the definition of those entities, and the timing of the draft’s passage and implementation, remain unclear.93

Under Article 40 of the Law No. 46/1999 on Post and Telecommunications, everyone is prohibited from intercepting information transmitted through any form of telecommunications channel.94 Yet there are 10 laws, including the ITE law, and 7 executive regulations which allow certain government or law enforcement agencies to conduct surveillance, including electronic surveillance over citizens.95 The agencies include the Indonesia Corruption Commission, the National Narcotic Board, National Intelligence Service, and others. However, the laws do not clearly explain the scope of interception, despite the fact that the Constitutional Court issued a decision in 2010 requiring that detailed interception procedures be regulated by law.96 In addition, the legal framework lacks judicial or parliamentary oversight, and does not provide a remedy for possible abuse.

Indonesia

In March 2015, reports based on information leaked by former U.S. National Security Agency (NSA) contractor Edward Snowden accused New Zealand of spying on digital communications in countries in the Pacific since 2009, including Indonesia going back to 2009.97 Many political figures and Indonesian officials asked for an official explanation from the New Zealand government.98 Separately, the same document alleged that SIM cards manufactured by the company Gemalto and used by telecommunication providers XL, Hutchinson 3, Telkomsel and Indosat were subject to surveillance by the NSA and the British intelligence agency GCHQ (Government Communication Headquarters). An official investigation found no supporting evidence of this claim.99

Intimidation and Violence

There have been no reports of extralegal attacks, intimidation, or torture of bloggers or other internet users. In the past, police—and sometimes Islamic fundamentalist groups—have conducted unannounced searches of cybercafes that are perceived to be promoting immoral conduct;100 no incidents were documented during the coverage period.

Technical Attacks

Politically-motivated cyberattacks against civil society groups have not been reported in Indonesia. A cyberattack allegedly initiated by Philippine hackers defaced several Indonesian websites in April 2015 as a protest against the planned execution of a Philippine national convicted of drug trafficking. She was ultimately granted a reprieve.101

The Minister of Defence reported recruiting experts and purchasing digital defensive tools to protect Indonesia from cyberattacks in May 2015.102

---

Iran

Key Developments: June 2014 – May 2015

- The ICT ministry’s budget reached its highest level in history, reflecting increasing investments in both internet infrastructure and censorship tools (see Availability and Ease of Access).

- An exclusive 3G contract issued to mobile operator RighTel was not renewed, thereby opening up licensing to all operators in a move that was not welcomed by the Supreme Council of Cyberspace and hardliners, who regard mobile internet as “un-Islamic” (see Regulatory Bodies).

- While the administration of President Hassan Rouhani did not fulfill campaign promises to unblock popular social media platforms, the government managed to change content blocking procedures to give government ministers more say over hardliners appointed by the Supreme Leader. This enabled the ICT ministry to push back against attempts to block chatting apps WhatsApp and Viber (see Blocking and Filtering).

- Several news sites were blocked throughout the year for publishing news on corruption or images of former political leaders that have fallen out of favor with the Supreme Leader (see Blocking and Filtering).

- In August 2014, Iranian cartoonist Atena Farghadani was arrested on charges of insulting state officials and spreading propaganda for posting an image of a parliamentary vote on reproductive rights. She was released in December, only to be rearrested one month later after uploading a video describing the abuse she faced at the hands of prison guards. She was sentenced to more than 12 years in prison in August 2015 (see Prosecutions and Detentions).

- In July and August 2014, authorities prevented an estimated 75 percent of users from connecting to Tor, an anonymous web-browsing tool used to evade censorship and surveillance (see Surveillance, Privacy, and Anonymity).
Introduction

Hassan Rouhani was elected president in 2013 promising to improve the lives of Iranians and ease restrictions on the use of the internet. The promises were particularly well received by Iranians, who during the final 18 months of former president Mahmood Ahmadinejad’s term saw conditions for internet freedom worsen. Upon the start of his presidency, the Rouhani administration increased the budget for SHOMA, Iran’s “national information network,” which aims to improve connectivity in Iran, while also enhancing the authorities’ ability to control the network and monitor citizens’ online activities. In a positive development, the Rouhani government made 3G licenses available to all mobile operators, creating the potential to diversify the market and increase access.

Rouhani’s administration has faced stiff resistance from hardliners demanding the maintenance of speed restrictions to prevent “un-Islamic behavior” and the filtering of messaging services such as WhatsApp and Viber. While Rouhani’s administration has successfully resisted some demands, many limits on content remain in place, and violations of user rights continue. In one case from July 2014, 8 Facebook activists were sentenced to a combined 127 years in prison for anti-government posts. In general, internet policy remains a contested space in Iran, with the hardliners viewing the internet as a threat to national security and favoring a “security-first” approach. Internet policy in Iran will continue to be shaped by differing state bodies, but like many other aspects of policymaking in Iran, the sector is ultimately controlled by the Supreme Leader, Ali Khamenei.

Despite these limitations, the internet remains the only viable means for Iranian citizens and dissenters to obtain news and organize themselves. Savvy users employ virtual private networks (VPNs) or other circumvention tools to access blocked content, turning to new services if existing ones are blocked by the authorities. This cat-and-mouse game largely continued over the past year.

Obstacles to Access

Most improvements to internet freedom that have come under the presidency of Hassan Rouhani relate to access and the ICT market. The ICT ministry’s budget reached its highest level in history, reflecting increasing investments in both internet infrastructure and censorship tools. National bandwidth increased by 2.5 times over the past year. The ICT ministry did not renew an exclusive 3G contract issued to mobile operator RighTel, thereby opening up licensing to all operators in a move that was not welcomed by the Supreme Council of Cyberspace (SCC) and hardliners, who regard internet-enabled mobile phones as “un-Islamic.”

Availability and Ease of Access

Statistics on the number of internet users in Iran are inconsistent and highly disputed, though most observers agree that usage continues to grow. According to the National Internet Development Management Center (MATMA), the national internet penetration rate was 49 percent in 2014-15,¹ which is lower than the figure of 61 percent that was reported by the same agency one year ago. The International Telecommunication Union (ITU) estimated the number of internet users in Iran at 39 percent of the population for 2014, up from 14 percent in 2009. Citing the Iranian Information

Iran

Technology Organization as its source, the ITU also said there are only 9.46 fixed-broadband subscriptions per every 100 inhabitants.  

Internet access in Iran remains relatively expensive considering the speed and quality of service, for two principal reasons. Firstly, the state-owned Telecommunications Infrastructure Company (TIC) holds an effective monopoly over the domestic bandwidth market, reselling bandwidth to ISPs. Mostafa Mohammadi, former secretary of Iran’s ISP Association, claimed the Telecommunications Company of Iran (TCI), one of the largest ISPs, buys internet bandwidth for under USD 1,000 and resells it to ISPs for around USD 11,300.  

Secondly, the demand for bandwidth is very high in the country, while its availability remains very low, due to political pressure.

There have been numerous promises by various officials to increase internet speeds. However, Iranian users are forced to endure some of the slowest connection speeds in the world. Even President Rouhani criticized Iran’s glacial internet speeds, joking that sometimes downloading an article takes so long that people fall asleep in front of their computers waiting for it to finish.  

According to Akamai, the leading global content delivery network, Iran has the world’s lowest average peak connection speed, at 6.0 Mbps.

Rouhani’s administration has stepped up efforts to implement SHOMA, the national information network, by bolstering the ICT Ministry’s budget to the highest it has ever been, with a large portion of the budget allocated to SHOMA. The Iranian government announced an investment of IRR 100,000-120,000 billion (USD 3.75–4.5 billion) to accelerate SHOMA’s completion, though it seems the development of SHOMA has been partially hampered by the government’s difficulties importing the required hardware from other countries. Nonetheless, SHOMA helped increase national bandwidth by 2.5 times in the past year, providing Iranians users with better speeds when trying to access websites hosted inside Iran. However, it has been stated that further increases in international bandwidth are conditional on the introduction of “intelligent filtering.”

Worryingly, SHOMA will create the infrastructure inside Iran that will allow the Iranian government to develop a national web ecosystem, while giving the authorities a better grip over the flow of traffic in Iran. Authorities hope that the development of a national web ecosystem will result in less reliance on international web services and will accordingly decrease the level of public discontent if major international web services are blocked. SHOMA will also increase the security of the state’s critical web infrastructure, in light of recent major cyberattacks against Iran. Officials from the government have even reached out to the Chinese government to enlist their help with its completion.

---

Restrictions on Connectivity

The Data and Communication Company (DCC), which operates under the Telecommunications Infrastructure Company (TIC), retains a monopoly on internet traffic flowing in and out of Iran. The TIC is a state-owned enterprise under the ICT ministry. The arrangement affords the Iranian authorities total control over the internet backbone, as well as the ability to limit access or throttle speeds during sensitive political moments, which last occurred in the lead-up to the 2013 presidential elections. The heavy influence of the TCI in the ICT market also grants the security apparatus the ability to control third-party ISPs and to monitor online activities, since the TCI’s majority shareholder is the Islamic Revolutionary Guard Corps (IRGC).

ICT Market

The telecommunications industry in Iran is tightly controlled by the government or related entities. In recent years, the role of the IRGC—a politically important branch of the security forces that also controls large sections of the economy—in the ICT sector has notably increased. In September 2009, for example, the IRGC purchased a controlling stake in the Telecommunications Company of Iran (TCI), the country’s main provider of internet and mobile phone services. Other providers must purchase bandwidth from the DCC. Direct access to the internet via satellite is only permitted for certain institutes and is prohibited for personal use. The mobile phone market is under similar state influence. IranCell, the second largest mobile operator behind the TCI, is owned in part by a web of proxy companies controlled by the IRGC and has a number of high profile IRGC ex-commanders among its management. The third operator, RighTel, was launched in early 2011. It, too, is a government-owned entity.

Meanwhile, cybercafes remain under the close scrutiny of officials. Five cybercafes have been shut down by FATA (North Khorasan Province) due to legal breaches. All cybercafes in Iran must follow a series of regulations such as engaging in CCTV surveillance, and keeping full records of all users’ internet activity.

Regulatory Bodies

There is no independent regulatory body for ICTs in Iran. The Communications Regulatory Authority (CRA), which falls under the ICT Ministry, is responsible for telecommunications licensing. Its head is appointed by the ICT minister. The CRA has taken several actions to improve quality of service and reduce prices for Iranian users, for example, by banning the TCI in Mazandaran province from selling internet services due to poor quality of service and overcharging. According to the CRA, ISPs in Iran have erroneously received IRR 17 billion (USD 646 million) from their customers as a result of miscalculations. The CRA also slashed the price of mobile data from IRR 2.5 to IRR 0.5 per kilobyte.
In a positive but confrontational move, the ICT ministry did not renew an exclusive 3G contract issued to RighTel, a mobile operator in Iran. This allowed other mobile operators to offer data services to their customers, increasing access to more Iranians. As a result, data traffic on TCI’s mobile network increased by 500 percent in the last year. However, the provision of 3G licenses to all the operators was not welcomed by the Supreme Council of Cyberspace (SCC), which complained that the ICT ministry did not ask for its permission to offer 3G licenses and stated that it would be illegal for the government to do so before further development of SHOMA. Naser Makarem Shirazi, one of Iran’s grand ayatollahs, branded high speed internet on mobile phones “un-Islamic,” arguing that the regulations and tools necessary to prevent corruption are not yet available. The Iranian parliament also threatened to impeach the ICT minister if internet speeds are increased prior to the launch of SHOMA.

The SCC was established by decree of the Supreme Leader Khamenei in March 2012. It is intended to provide a centralized focal point for policymaking and the regulation of Iran’s virtual space, effectively minimizing the roles of the executive, legislative, and judicial branches of the government and bringing it under Khamenei’s direct control. Observers believe this reflected Khamenei’s dwindling trust in former president Mahmood Ahmadinejad to lead such an important area of policy.

**Limits on Content**

Significant limits on content remain in place. While the administration of President Hassan Rouhani has not fulfilled campaign promises to unblock popular social media platforms, the government has succeeded in changing procedures behind the blocking of content to give government ministers more say over hardliners appointed by the Supreme Leader. In another positive move, the ICT ministry successfully pushed back against attempts to block chatting apps WhatsApp and Viber. Nonetheless, several news sites were blocked throughout the year for publishing news on corruption or images of former political leaders that have fallen out of favor with the Supreme Leader. The high level of self-censorship and the blocking of social media continued to stymie any significant digital activism.

**Blocking and Filtering**

The Iranian authorities continued to restrict access to tens of thousands of websites in 2014-2015, particularly those of international news sources, the opposition, ethnic and religious minorities, and human rights groups. Websites are also filtered if they differ from the official doctrine of the state’s Islam.

The mobile messaging app WhatsApp became a symbol of the power struggle between hardliners and President Rouhani’s government. On April 30, 2014, the CDICC ordered the ICT Ministry to block WhatsApp. Shortly afterwards, ICT Minister Mahmoud Vaezi announced that the proposed blocking of WhatsApp had been suspended by President Hassan Rouhani. According to Vaezi, President Rou-

---

Iran

hani considers the Supreme Council of Cyberspace (SCC) responsible for managing policy relating to social networks, while the CDICC is an administrative committee that implements policy. CDICC Secretary Abdolsamad Khoramabadi responded by stating that the president does not have the power to suspend the CDICC’s orders, and insisted that the Rouhani government must execute the committee’s rulings. Vaezi pointedly remarked that Khoramabadi is merely the secretary of a committee, and that he has no authority to issue orders to either the President, or to the SCC.20 As the result of this standoff, WhatsApp and Viber have remained accessible.

Meanwhile, popular social networks such as Twitter and Facebook remain blocked in Iran. Despite Rouhani’s promise to unblock social networks during his campaign, the ICT minister has denied the claim, while emphasizing the need for private companies and universities to develop domestic social networks for Iranians. He went on to point out that filtering is not the responsibility of his ministry; rather, it falls under the purview of the CDICC. This contradicts an earlier statement made by Vaezi but reflects how the Rouhani government has evaded responsibility for the unblocking of popular social networks.21

Iran continues to block some major international news websites, such as the BBC, as well as Persian news websites based outside of Iran. News websites based in Iran continue to operate in a very restrictive environment, which occasionally results in filtering actions. A few examples include:

- On September 4, 2014, the news agency Dana was blocked after publishing a news article about corruption allegations facing former IRGC commander Mohammad Rouyanian. Rouyanian was arrested on May 6, 2014 and charged with financial corruption and money laundering.22
- On September 30, 2014, Salam Noo was blocked by the General Prosecutor of Tehran, without any explanation. Launched in August 2014, the website is close to the minority Islamic Kar Party.23
- On February 27, 2015, Jamaran, the website that covers news of former supreme leader Khomeini’s family, and Bahar News were blocked after publishing a photo of former president Khatami, who is banned from receiving any publicity. Both sites were unblocked after removing the photo.24

Internet traffic over cell phones is subject to a similar level of restrictions as fixed-line connections. Iranians are barred from making video calls on their mobile phones due to the concern that this technology will bring about “cultural damage.”25 Similarly, dating websites have also been blocked after FATA announced that all dating websites in Iran are illegal and lack permission to operate.26 Clash of Clans, a popular game amongst Iranians, has been blocked without explanation. According

---

Iran

to Iran Clash, users have seen connection error message when trying to play it on their phones and tablets.\textsuperscript{27} Iranian mobile users have only intermittent access to major app stores such as Apple’s iTunes or Google Play, either due to blocking by the Iranian government (in the case of the former) or by the providing company (with regard to the latter).

SMS content is also subject to filtering. For instance the term, “come to eat” was blocked by IranCell in July 2014. The term is an everyday phrase in the Persian language, though it also has sexual connotations when used colloquially. During the election period, SMS messages containing the word “Mashaei” were blocked, referring to Esfandiar Rahim Mashaei, the presidential candidate supported by Ahmadinejad. Texts containing political slogans related to Mashaei and Ahmadinejad have also been blocked in the past.

Currently there is no legal framework for filtering SMS content. However, in June 2013, the SCC’s director announced that it will work with the Ministry of Culture and Islamic Guidance to draft a new bylaw for monitoring the content of mass and promotional text messages.\textsuperscript{28} The CRA has also introduced new regulations that require all commercial SMS senders to submit the content of each SMS or service to the CRA for review prior to sending.\textsuperscript{29}

Iranian authorities currently employ a centralized filtering system that can effectively block a website within a few hours across the entire network in Iran. Private ISPs are forced to either use the bandwidth provided by the government or route traffic containing site-visit requests through government-issued filtering boxes developed by software companies inside Iran. The filtering boxes search for banned text strings—either keywords or domain names—in the URL requests submitted by users, and block access accordingly.

Internet filtering, which began toward the end of the Khatami presidency in 2005, has become more severe since the disputed presidential election in June 2009. Calls for an “intelligent filtering” system, using a technique known as deep-packet inspection (DPI), continue to be announced by various officials in order to allow for the blocking of specific pages within a site rather than blocking the entire site. There have been a number of vague announcements that some parts of this system have been launched, but no specific details have been provided. The system would “recognize” URLs and block a specific part of the address, rather than the entire domain. The system would also define different access levels for various users. For instance, students would have a specific level of access so that they can conduct research for their papers. It has also been announced that the system would analyze videos, images, and audio files, and decide which ones to block. Analyzing multimedia content or encrypted content (HTTPS) will be technically very resource intensive, if not impossible. For instance, after the ICT minister announced that intelligent filtering had been successfully applied to Instagram, Instagram enabled a default SSL encryption on its entire platform, resulting in blocked pages becoming available again.\textsuperscript{30}

In an effort to show that content filtering is based on a legal framework, institutions to oversee internet filtering have been created. The Committee for Determining Instances of Criminal Content (CDICC) is empowered to identify sites that carry forbidden content and report such information to the TCI and other major ISPs for blocking. The committee is headed by the prosecutor general, and

\begin{itemize}
  \item \textsuperscript{27} “Problem with entering to Clash of Clans,” [in Farsi] IranClash, accessed on March 29, 2015, http://goo.gl/LdVC4r.
\end{itemize}
Iran

its members are representatives from 12 governmental bodies. Little information is available about
the inner workings of the committee, and censorship decisions are often arbitrary and nontrans-
parent. According to the law, the committee should meet biweekly to decide on any website bans,
though the bulk of filtering decisions are likely made upon discovery of objectionable content, or by
a small technical team. In addition, owners of websites registered with the Ministry of Culture have
complained that they received no explanation when their websites were filtered. The authorities
claim there is a procedure for disputing filtering decisions. However, the process is highly inefficient,
and even conservative bloggers have failed to have their webpages unblocked by lodging com-
plaints. Moreover, the dispute process requires the website owner to disclose his or her personal
information and accept responsibility for any misconduct in the future, a commitment that few are
willing to make given the risk of severe punishment.

Since taking office, the administration of President Hassan Rouhani has sought to assume more
direct control over ICT policy in Iran. However, such moves have been met with fierce opposition
from hardliners. Sadeq Larijani, head of Iran’s judiciary, indirectly criticized Rouhani’s internet policies,
warning that Iranian authorities should be cautious about issues relating to communication, cyber-
space, and cultural affairs. Larijani warned politicians against employing excited or emotional lan-
guage on these issues. He emphasized that the main decision-maker regarding internet censorship
in Iran is the CDICC, not the government, and highlighted that the law determines which websites
and services must be blocked.

Such reactions have prevented Rouhani from achieving any broad policy change, though he has
been able to achieve some limited successes. For instance, Rouhani oversaw a change in the voting
procedure by which the CDICC blocks websites. Previously, the decision to block a website or service
required the support of just 5 members of the committee in a vote, but now an absolute majority
of all 13 members is required. Such a change gives more power to Rouhani’s administration as the
majority of its 13 members are government ministers.

Content Removal

Aside from filtering, Iran also employs administrative measures to remove unwanted content from
the web. Website owners must register their sites with the Ministry of Culture and are then subject
to requests to remove particular posts deemed unacceptable by the government. The 2009 Compu-
er Crime Law (CCL) makes service providers, such as blogging platforms, responsible for any content
that appears on their sites. This has led to the suspension of blogs or shuttering of news websites
hosted on platforms inside Iran, under orders from government officials. The CCL also specifies vio-
lations that might result in a website being marked for filtering. These are defined very broadly and
range from insulting religious figures and government officials to distributing pornographic content
and the use of illegal circumvention tools.

34 “The monopoly of filtering decisions by 5 individuals has been broken,” [in Farsi] ITMen, accessed March 29, 2015, http://
bit.ly/1hEO03A.
media/library/2921/12-01-30-FINAL-iran-WEB(4).pdf and “12 members of Committee in Charge of Determining Unauthorized
While complaints about censorship have typically come from reformist and independent media, activists from semiofficial news agencies and conservative websites appear to have been contacted by the CDICC and asked to “either remove specific text from their website or risk filtering.” Critics say the committee does not have the jurisdiction to deal directly with websites and news agencies that are licensed by the Press Supervisory Board.36

**Media, Diversity, and Content Manipulation**

Self-censorship is extensive, particularly on political matters. Widespread arrests and harsh sentences meted out to reporters and activists after the 2009 elections, as well as perceptions of pervasive surveillance, have increased fear among online journalists and bloggers. Many either abandoned their online activities or used pseudonyms, resulting in a palpable drop in the amount of original content being produced by users based inside the country. However, the situation slightly improved after Rouhani assumed the presidency, especially among reformist journalists who advocated for him. Nevertheless, the same restrictions of the pre-Rouhani era are still in place, and journalists continue to be prosecuted.

In addition to filtering, censorship, and intimidation, the state counters critical content and online organizing efforts by extending regime propaganda into the digital sphere. There are at least 400 news websites either directly or indirectly supported by the state. They seek to set the agenda by providing progovernment commentary or publishing rumors. There have also been a large number of government-backed initiatives to promote blogging among its supporters and members of the Basij paramilitary group.37

Furthermore, the majority of independent content producers lack the financial resources to operate in such a hostile environment. The online advertising market in Iran is exclusively limited to apolitical and progovernment websites. Even businesses based outside Iran avoid political websites to maintain trading relationships with the country. Although the United States adjusted its sanctions against Iran to enable American internet companies to provide services to Iranian users, Google Advertising does not recognize Persian as one of the languages in its system, disadvantaging Persian content producers.38 Any Iranian-linked company or individual who wishes to use Google AdSense must apply for a specific license, which is not a convenient process for the majority of Iranian content producers.

In August 2014, Rouhani’s administration announced the creation of the Freedom of Information Commission (FOIC), which will be headed by the Minister of Culture and Islamic Guidance. The groundwork for the FOIC was laid during Ahmadinejad’s presidency. It is yet to be seen how FOIC will function in practice, but in theory, the FOIC will allow all Iranians to access public information from all the governmental entities, unless prohibited by law. Also, all organizations that fall under the control of the Supreme Leader, such as the IRGC, must receive the minister’s permission prior to publishing information.39

---

Iran

Iranian authorities actively support Iranian social networks and mobile app developers by offering free bandwidth and hosting, with the aim of attracting Iranian users to these platforms over those based outside of Iran. Currently, there are 20 Iranian social networks operating in the country, but none have become popular. Efforts to suppress foreign technology suggest a general alignment with the internet policies of China, which has undertaken a similar purge of Western-produced applications, while promoting home-grown variants that appear to be part of an effort to simplify state monitoring of private communications and limit citizens’ access to information.

Meanwhile, the Iranian government continued its cat-and-mouse game against the use of circumvention tools during the coverage period. The use of such tools is considered illegal, although many ignore this. According to the most recent statistics, 45 percent of Iranian users utilize VPNs to bypass censorship, and 41 percent use other circumvention methods to access blocked content.

Digital Activism

Due to the ongoing blocks on Facebook and Twitter, opposition campaigning on Persian social media is limited in reach and scope. However, Facebook remains the most effective platform for the engagement between those based inside and outside of Iran. In February 2015, when Iran’s federal prosecutors announced that it was illegal for the media to publish photos or news about former president Mohamed Khatami, Iranians users promptly launched an online campaign titled, “We are Khatami’s media,” on Facebook, reaching nearly 30,000 “likes” in 24 hours. Many of them published photos of him under multiple hashtags, challenging the official ban.

Violations of User Rights

An undemocratic legal environment, harsh prison sentences, and rampant surveillance impede the rights of internet users in Iran. Several individuals were imprisoned for nonviolent speech that met the ire of authorities. Cartoonist Atena Farghadani was sentenced to more than 12 years for a YouTube video, eight young Facebook users received a combined 127 years for, and tech bloggers were handed 11 years each. At the same time, authorities have made it more difficult to evade censorship and surveillance by restricting access to popular circumvention tools.

Legal Environment

Iran continues to be an extremely dangerous environment for internet users. Iranian laws heavily restrict what is acceptable speech online and specify harsh punishments for those who deliberately flout restrictions, as well as those who have inadvertently drawn the ire of authorities. The constitution provides for limited freedom of opinion and expression, but numerous, haphazardly enforced laws restrict these rights in practice. The 2000 Press Law, for example, forbids the publication of

ideas that are contrary to Islamic principles or detrimental to public rights, none of which are clearly defined. The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize critical opinions.

The 2009 CCL outlines punishments for spying, hacking, piracy, phishing, libel, and publishing materials deemed to damage “public morality” or to be a “dissemination of lies.” Punishments are severe and include the death penalty for offenses against public morality and chastity, as well as long prison sentences, draconian fines, and penalties for service providers who fail to enforce government content restrictions.44

**Prosecutions and Detentions for Online Activities**

Despite President Hassan Rouhani’s progressive views on accessing social networking sites, his voice has remained silent as Iranian internet users faced increasing arrests and severe punishments.45 During the coverage period, a number of users were arrested and imprisoned for their online activities, particularly for posts on social media sites that are officially blocked within the country. As of mid-2015, Reporters Without Borders reports that 26 netizens remain imprisoned for online activities.46

Among the arrested were bloggers and journalists working at online publications:

- Mohammad Reza Pourshajari (aka Siamak Mehr), a blogger, was detained in September 2014 for criticizing the Islamic Republic and Islam on his blog Gozaresh be Khaak-e-Iran (Reports to the Soil of Iran).47
- Ali Ghazali, the managing editor of two news websites Baztab Emrooz and Ayandeh Online, was arrested and charged with “publishing lies with the intent to create public anxiety” in November 2014. Ghazali published articles on alleged government corruption.48

Iranian courts also issued draconian prison sentences in an attempt to clamp down on any online content that is critical of the state.

- In August 2014, Iranian cartoonist Atena Farghadani was arrested on charges of insulting state officials and spreading propaganda for posting an image of a parliamentary vote on reproductive rights, in which she depicted members of parliament as animals. She was released in December, only to be rearrested one month later after uploading a video describing the abuse she faced at the hands of prison guards. She was sentenced to more than 12 years in prison in August 2015.49
- In July 2014, 8 youths were sentenced by a revolutionary court to a combined 127 years for

---

antigovernment posts on Facebook.\(^\text{50}\) Many of the sentences were reduced in early 2015, although they remain between five and seven years for charges of insulting the Supreme Leader and state officials as well as “propaganda against the state.”\(^\text{51}\)

- Even apolitical tech bloggers for the Iranian gadget news site Narenji were arrested in 2013 for attempting to overthrow the Iranian regime and sentenced to 11 years each in jail in June 2014.\(^\text{52}\)

In March 2015, the Cyber Intelligence Unit of the IRGC reported that it had arrested 12 individuals and summoned 24 others on charges such as “insulting Islam,” “publishing immoral and corrupt material,” and “encouraging individuals to commit immoral acts.” The arrests came after a surveillance operation in which the IRGC claimed to have analyzed eight million Facebook “likes” to crack down on content that promoted “moral corruption” or Western lifestyles.\(^\text{53}\) One user, a university student, was reportedly accused of managing some 20 Facebook pages containing “immoral” content.

### Surveillance, Privacy, and Anonymity

The online sphere is heavily monitored by the state in Iran. Both FATA and the ICT Ministry have announced that they are capable of monitoring all messages sent on messaging apps Viber, Tango, and WhatsApp.\(^\text{54}\) However, it remains unclear how the authorities can technically monitor the content of messages, given that some of these apps encrypt their messages. All platforms and content hosted in Iran are subject to arbitrary requests by various authorities to provide more information on their users. Local equivalents of international platforms do not guarantee an adequate level of protection for users. For instance, a replica of Facebook, Facenama, was hacked, resulting in the leaking of the personal information of all of its users in December 2014.\(^\text{55}\)

The expansion of SHOMA further threatens to infringe on users’ privacy in Iran, such as a proposal to require all internet users to log-in with a unique ID to browse the internet. The government claims the IDs are needed to fight corruption;\(^\text{56}\) however, such functionality will also enable the authorities to find out the real identities of online users and target them for their online activities.

The Iranian government can easily block encrypted traffic. In July and August, the Iranian government prevented an estimated 75 percent of the network’s users (about 40,000 daily) from connecting to Tor, an anonymous web-browsing tool used to evade censorship and surveillance.\(^\text{57}\)


\(^{57}\) Kyle Bowen and James Marchant, “Internet Censorship in Iran: Preventative, Interceptive, and Reactive,” in 436
Iran

Intimidation and Violence

Extralegal intimidation and violence by state authorities is prevalent in Iran. In 2012, blogger Sattar Beheshti was killed while in prison. Groups such as the IRGC are known to pressure social media users to delete content. For example, the IRGC announced in February 2015 that it had deleted 130 Facebook pages managed by 36 individuals since September 2014, which observers believe were deleted by the page owners while under coercion, given that Facebook does not have a relationship with the Iranian government.\textsuperscript{58}

Technical Attacks

Hacking continues to be the most popular tool at the hands of Iranian authorities to target Iranian activists and foreign governments alike. In mid-2014, the network security group FireEye published a comprehensive report on “Operation Saffron Rose,” a hacking operation by the Iranian hacker group “Ajax Security Team.” According to the report, hackers have quickly advanced from website defacements and DDoS attacks to “malware-based espionage.” The hacking team has also created decoy installers for various circumvention tools, including Ultrasurf, Gerdoo VPN, Psiphon and Proxifier, thereby targeting Iranian users as well as foreign entities.\textsuperscript{59}

Italy

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>22</td>
<td>23</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 61.3 million
Internet Penetration 2014: 62 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2015 Status: Partly Free

Key Developments: June 2014 – May 2015

- In the wake of terrorist attacks in Paris, Italy passed an antiterrorism law in April 2015 that criminalized online terrorist recruitment and the endorsement or incitement or terrorism online (see Legal Environment).

- The antiterrorism law also entrusts the public prosecutor with drawing up a blacklist of terrorist websites to be blocked or taken down by service providers, without including provisions for judicial oversight (see Blocking and Filtering and Content Removal).

- Service providers must also retain user metadata for a period of 24 months, up from 12, despite a European court ruling that such measures restricted the fundamental right to privacy one year earlier (see Surveillance, Privacy, and Anonymity).

- An interparliamentary committee, appointed in July 2014, released a nonbinding “Declaration of Internet Rights” in a bid to increase awareness of digital rights and to inspire legislative actions (see Legal Environment).
Introduction

For a country with an advanced economy, Italy’s internet penetration rate lags behind that of many other European countries at around 62 percent of the population. Italian authorities do not generally engage in political censorship of online speech, and, as in previous years, no bloggers or social media users were imprisoned as of mid-2015. One of the most significant developments during the coverage period was the passage of a new antiterrorism law in April 2015. The law broadened language in the criminal code on terrorist recruitment as well as the endorsement or incitement of terrorism to include online offenses. The law also provides for the blocking and removal of terrorist websites by order of the public prosecutor, who may request ISPs prevent access to a blacklist drawn up by the Interior Ministry. Regarding surveillance, the law extends the period that internet providers must retain user data to 24 months, despite the Court of Justice of the European Union striking down the European Data Directive in April 2014. On a positive note, an article authorizing the police to remotely access targets’ computers was withdrawn from the antiterrorism law.

Several other legal developments took place over the past year. A proposed tax on e-commerce, commonly dubbed as a “Digital Tax” or “Google Tax,” may be revived after Prime Minister Matteo Renzi’s recent comments in favor of the shelved bill. The proposal would impose a 25 percent tax levy on multinational companies selling digital services and operating longer than six months in Italy with revenues of over 5 million euros. Italy’s Transportation Authority has introduced a proposal to change the regulation of public transportation in a bid to accommodate ride-sharing services such as Uber, a popular mobile app which had been plagued by legal obstacles. Finally, Italy became the first European country to publish a “Declaration of Internet Rights” after an interparliamentary committee released the document for further public consultation. The declaration is not legally binding, but experts and activists hope it will be taken up by legislations when amending the country’s current set of laws.

Italy’s first computer network emerged in 1980, when a group of nuclear physicists connected all of the country’s nuclear research institutes. At the beginning, the internet was just one of several packet-switching networks that coexisted in Italy. The dominant telecommunications firm at the time, Telecom Italia, tried to impose its privately owned system, while various center-left governments, aware of the importance of interconnectivity, supported integration among the networks. Ultimately, the adaptability and simplicity of the internet prevailed. Access to the internet was available to private users after 1995, and the number of internet service providers (ISPs) soared within a short period of time. Among the remaining obstacles to greater internet penetration include a lack of familiarity with computers and with the English language, as well as the dominance of commercial television, and the diversion of consumers’ telecommunications spending to mobile telephony. Since the February 2013 elections, the use of social media and the web has proved to be a central element of political communication.

Obstacles to Access

Since the 1990s, the Italian government has supported the internet as a catalyst for economic growth, increased tourism, reduced communication costs, and more efficient government operations. As of 2014-15, this attitude still prevails but, as in the past, there is a considerable gap between aspirations and reality.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), Italy had an internet penetration rate of 62 percent in 2014, an increase from 49 percent in 2009. While Italy’s internet penetration rate is higher than the global average, it is much lower than the overall rate in Western Europe and, as indicated by a recent report, it lags behind in many ICT indicators in Europe. The relatively low penetration rate is only partially due to infrastructural limitations, as unfamiliarity with the internet among the older generations as well as a penchant for mobile phone devices rather than desktop computers also contribute. Naturally, Italy’s most devastating financial crisis in its modern history has something to do with it as well.

Mobile phone use is much more widespread than internet access, with the penetration rate reaching 154 percent in 2014. The majority of subscriptions are still prepaid, but flat tariffs are quickly on the rise. Mobile telephone usage is ubiquitous, however, and internet access via mobile phones is almost dominant now. Mobile access now accounts for well over 60 percent of internet users. For fixed lines, Italians still prefer to access from home, with the workplace the second most common access point, followed by schools and universities. Slightly less than half of Italy’s internet users are female.

Cost is not a significant barrier to access. The price for a broadband connection may range from €20 to €40 (US$26-52) per month, compared to average monthly per capita income of around US$2,700.

ADSL (fixed) broadband connections (which reach up to 2 Mbps when advertised as “basic service”) are available in about 98 percent of Italy’s territory. However, fast broadband (more than 30 Mbps) is only slated to reach 50 percent of the territory in 2016-17. Italy has one of lowest coverage rates of high speed broadband in the EU, with only 21 percent of households covered compared to a European average of 62 percent. At the end of 2014, the average speed of connections in Italy was 5.6Mbps, with only 5.7 percent of Italians enjoying speeds over 10Mbps (albeit with a growth of 28
percent compared to 2013). There is no plan by telecom companies to achieve ultrafast broadband (over 100 Mbps) anytime soon.

The ambitious infrastructural plan, “Growth 2.0”, was announced in 2012 to close Italy’s digital divide between those areas that are served by high-speed connections and those that are not by 2014. In February 2014, however, the goal was delayed to 2015, albeit as of mid-2015 no further update has appeared. The same document also launched the “Digital Agenda” initiative (based on the EU Agenda 2020), intended to expand broadband access and e-government functions (including “digital identity,” public e-services, “intelligent communities,” and so on). The then-prime minister Enrico Letta appointed Francesco Caio (whom Letta nicknamed “Mr. Digital Agenda”) as the government’s commissioner in June 2013. Caio, a manager with a long experience in telecom, presented a comprehensive report in January 2014; the infrastructure and economic development minister, along with several other ministries (economy, research and university, public health and others) were meant to be involved in the realization of the digital agenda that would profoundly “transform” Italy’s public administration. Then the government changed, Caio left to become Poste Italiane’s CEO and the project was inevitably put on hold. Current Prime Minister Renzi has again emphasized the centrality of the digital agenda, but with this stop-and-go Italy is unlikely to fulfill the EU goal.

Restrictions on Connectivity

The government does not impose restrictions on ICT connectivity and access to social media and communication platforms. Telecom Italia owns the physical network, but it is required by European Union (EU) legislation to provide fair access to competitors. Telecom Italia began the process of “externalizing” the infrastructure at the end of May 2013.

ICT Market

Access to the internet for private users is offered by 13 different ISPs. Telecom Italia has the largest share of the market, followed by Vodafone, Fastweb, and Tiscali. Telecom Italia Mobile (TIM), Vodafone, Wind, and 3 Italia are the major carriers, and all of them operate third-generation (3G) networks. As elsewhere, sales of tablet computers have been on the rise among the younger generation since 2010 and are likely to keep growing in the coming years.

Regulatory Bodies

The main regulatory body for telecommunications is the Authority for Communications (AGCOM), an independent agency that is accountable to the parliament. Its responsibilities include providing access to networks, protecting intellectual property rights, regulating advertisements, and overseeing

15 Achieving the Objectives of the Digital Agenda for Europe (DAE) in Italy: Prospects and Challenges. The six “strategic areas of the "Digital Agenda" include infrastructure and cyber security, e-commerce, e-government, e-learning (e-books, digital policy literacy and e-participation), research and innovation in ICT, and smart cities and communities.
Italy

public broadcasting. The parliament’s majority party appoints AGCOM’s president. It used to be that commissioners would come under pressure when it came television broadcasts, (particularly during Berlusconi’s premiership), but today digital copyright is the agency’s “beite noire,” with a proposal for taxing all electronics products. AGCOM’s current president Angelo M. Cardani, appointed in July 2012, is in fact a staunch supporter of the regulation that allows the agency to act in first person in case of copyright infringement.\textsuperscript{17}

Another important player in the field of communications is the Italian Data Protection Authority (DPA). Set up in 1997, the DPA today has a staff of more than 100 people, and four of its main members are elected by parliament for seven-year terms. The DPA is tasked with supervising compliance by both governmental and nongovernmental entities with data protection laws, and “banning or blocking processing operations that are liable to cause serious harm to individuals.”\textsuperscript{18} It is generally viewed as professional and fair in carrying out its duties. In April 2014, the authority launched a public consultation to assess public support for a large database (SIT, Sistema Informatico Integrato) on “bad payers” for telecom companies, which can consult it before accepting a new customer.\textsuperscript{19} There are clearly privacy issues involved, which is the rational for the consultation.

Limits on Content

\textit{Authorities do not engage in significant blocking or filtering of internet content, although recent measures to block illegal materials without a court order have worried digital rights activists. Italians have access to the full range of domestic and international news sources and human rights websites. Indeed, a research published by AGCOM on “Internet and Information in Italy” and in April 2015 showed that, although television still represents the first source of information for most Italians, the web and social networks come in second.}

Blocking and Filtering

Italy does not block or filter content of a political, social, or religious nature. However, certain websites related to gambling, copyright infringement, and terrorism are subject to blocking or removals (see “Content Removal”). The social-networking site Facebook, the Twitter micro-blogging service, the video-sharing site YouTube, and international blog-hosting sites are all freely available.

Since 2006, online gambling has been permitted only via state-licensed websites, and ISPs are required to block access to international or unlicensed gambling sites identified on a blacklist compiled by the Autonomous Administration of State Monopolies (AAMS). The list of banned sites is available on the AAMS website and updated regularly.\textsuperscript{20} A similar blacklist system is in place for websites containing child pornography. A law passed in February 2006 (Law No. 6) called for the establishment of a National Center for the Fight against Child Pornography on the Internet within the Postal and Communications Police Service. Based on its own research and on complaints from citizens, the center maintains a list of sites deemed inappropriate and forwards it to ISPs for block-

\begin{footnotesize}
\begin{itemize}
\item Cardani is a former chief of staff of Mario Monti when the latter was EU Anti-Trust commissioner. He also worked within the EU Commission for a while; See, AGCOM, "Componenti," http://bit.ly/1Mnsuss.
\item The blacklist is available (in Italian) at http://www.aams.gov.it/site.php?id=2484.
\end{itemize}
\end{footnotesize}
Italy

As with the AAMS list, the child pornography blacklist is publicly available, though some child advocates have raised concerns that this encourages visits to the sites by users with circumvention tools. ISPs also offer subscribers “family internet” packages that block access to adult pornography and sites with violent content, in exchange for a small premium.

Decisions related to the blocking of websites for copyright violations are implemented by the Guardia di Finanza (Finance Guard or GdF), which handles issues of cybercrime, fraud, and trafficking. In the infrequent cases in which websites containing news have to be blocked for copyright, this is made possible by a 1941 law, explicitly amended by the Berlusconi government in 2005 to include the web and computer communication.

In October 2011, the European Court of Justice had ruled that soccer games could not be protected by copyright, and the same year, a Rome court ruled against RTI (a subsidiary of the Berlusconi-owned Mediaset) that tried to prevent Google’s Blogger platform from streaming Italian football matches from Mediaset’s TV channels. Nevertheless, in early 2013 a court in Milan ruled that, even if the soccer game itself was not protected, distributors could seek copyright protection over its broadcast. Thus RTI-Mediaset won the case and ten indexing platforms with links to the streaming of major sports events were shut down. This decision was reiterated again in September 2013 by a court in Rome that ruled that link to soccer game streaming cannot be justified on the basis of freedom of the press because it is a copyright violation, thus accepting Mediaset’s viewpoint against the webzine Il Post.

The 2014 antiterrorism law (voted in the Senate on April 15) also provides for the blocking and removal of terrorist websites by order of the public prosecutor, who may request that ISPs prevent access to a blacklist drawn up by the Interior Ministry similar to that used to block child pornography sites.

Content Removal

Provisions for the removal of content have taken center stage in recent years. In December 2013, AGCOM finally adopted the highly controversial resolution that gives it the power to remove content upon review by an internal panel but without prior judicial approval, if a copyright violation is detected. The resolution, which had strongly been criticized by users’ organizations and ISP representatives, entered into force on March 31, 2014. In April 2014, the first procedures for violations of


22 The Italian Police, acting on order by a judge in Rome, who ruled in favor of a film distribution company (Sunshine Pictures), ordered 27 Italian and international ISPs to proceed with a DNS blockade to prevent Italian users to see a French movie “Un Monstre à Paris” distributed by the company. Mauro Vecchio, “Italia, maxisequestro dello sharing in corso,” Punto Informatico, April 15, 2013, http://bit.ly/1L8STCA.


26 Sghirinzetti, “Italy: Anti-terrorism decree to strengthen government surveillance.”


Italy

copyrights by foreign hosts began, and the problematic construction of the resolution was fully revealed. Previous laws from 2000 and 2003 gave AGCOM an executive mandate to act to take down violations of copyrights.29

The most controversial aspect is that on the basis of an administrative order by AGCOM, after the relevant investigation, ISPs can inhibit access to specific websites, even those that simply contain links through which it is possible to download content that is copyright protected. In May 2014, the authority granted Italian ISPs the mandate to block access to foreign websites that did not reply to AGCOM’s solicitations on the basis of the order that would “eventually” arrive.30 This posture would give ISPs a highly discretionary power, without a judicial order or ruling, to filter access to websites. Furthermore, in so doing, ISPs would impede users’ access to other legal links and content hosted by those web sites.

Based on these concerns, consumers’ organizations and ISP associations appealed the resolution, and in April 9, 2014 Rome’s administrative court ruled that opposition to the resolution was justified and asked AGCOM for a moratorium until June 2014 for further consideration and examination. The authority, however, decided to proceed and run the risk that, after a future contrary ruling, its executive decisions may all be void and unlawful.31

At times, Italian authorities continue to request the removal of specific content, though the amount is limited. According to Google, the government issued 65 requests for content removal between July and December 2013 (compared to 33 over the previous six months), a considerable increase.32 77 percent of the requests were broadly interpreted as “defamatory”. Finally, a draft bill being introduced in parliament in March 2015, as part of new anti-terrorism law, may affect ISPs as well, because, if passed, it would oblige ISPs to remove controversial material (especially hate speech).33

Foreshadowing the European Union ruling in favor of the so-called “the right to be forgotten” (or “right to oblivion”), in April 2012, the Italian Supreme Court imposed an obligation on publishers to update their online archives to ensure that outdated facts do not inadvertently damage someone’s reputation. But the court also pointed out there were no grounds for libel against the online news outlet that posted the story because events recounted in the article were true, even if they were incomplete or outdated. Routinely, bill proposals to exacerbate the current law and punish bloggers more harshly are presented in parliament, albeit they do not go much farther than that.34

Because of Italy’s civil-law system, some judges may occasionally still issue rulings imposing responsibilities on intermediaries to regulate user-generated content, though, judges have repeatedly affirmed that intermediaries should not be liable for the content posted by users. Many in the Italian legal community now believe that, based on existing jurisprudence and thanks also to the provisions laid out in the European Union (EU) e-Commerce Directive,35 service providers should not be

---

Italy

required to censor search results. Likewise, at the end of 2011, Italy’s Supreme Court declared that editors of online magazines were not responsible for defamatory comments posted by readers (thus taking into account the difference between the printed and electronic press). Attempts at introducing bills that would require websites to engage in pre-publication censorship have mostly stalled. At times, proposals that raised alarm bells for free expression advocates have been put forward by past governments (with Berlusconi’s being the most determined), but nothing has come out of them.36

Media, Diversity, and Content Manipulation

Even in the absence of legal requirements, ISPs tend to exercise some informal self-censorship, declining to host content that may prove controversial or that could create friction with powerful entities or individuals. Online writers also exercise caution to avoid libel suits by public officials, whose litigation—even when unsuccessful—often takes a significant financial toll on defendants in the traditional media. The Italian government does not proactively manipulate news websites.

Blogging is very popular in Italy, though television remains by far the leading medium for obtaining news. Most policymakers, popular journalists, and figures in the entertainment industry have their own blogs, as do many ordinary citizens. Social-networking sites, especially Facebook and Twitter, have emerged as crucial tools for organizing protests and other mass gatherings, such as concerts, parties, or political rallies, although, at times, some content may be aggressive. It is now “mandatory” for all parties to be adept at communicating via Facebook, Twitter and other social media.

Some restrictions on internet content uncommon in other Western European countries remain in place in Italy. Drawing on a 1948 law against the “clandestine press,” a regulation issued in 2001 holds that anyone providing a news service, including on the internet, must be a “chartered” journalist within the Communication Workers’ Registry (ROC) and hold membership in the national journalists’ association.37 With the exception of one case from late 2000s, these rules have generally not been applied to bloggers and, in practice, millions of blogs are published in Italy without repercussions. Nonetheless, many people who create websites on a range of issues (including scholarly research) still continue to collaborate with registered journalists to protect themselves from potential legal action.

Digital Activism

The use of social media and the web in the general elections of February 2013 proved to be a major innovation. Online tools were central, not only as a communication medium, but also to measure political sympathies by measuring “likes”, hashtags and tweets for the many political players.38 The Five Star Movement, a political party led by former comedian Beppe Grillo, based their political campaign almost exclusively on the internet and declined to take part in political talk-shows or television interviews.

As soon as the new parliament was in office, following the February elections, Grillo and his move-

---

36 In previous years one blog dealing with a sensitive criminal trial had been shut down, but that has been an exception rather than the rule.
The Five star Movement used the web and social media to: (1) select a candidate as the new president of the Italian republic,\(^{39}\) (2) vote on expulsion from the movement/party of those MP who did not conform to the movement’s rules and internal decisions, and (3) provide an outlet for Grillo’s announcement and statements.\(^{40}\)

Finally there has been a considerable talk about adopting an FOIA provision for Italy’s public administration (PA), modeled on the American act. Yet a comparison between the Italian (Law n. 241/1990) and U.S. legislation shows that, in the Italian case, open data is mostly a declared “intention” as opposed to a real, sanctioned obligation.\(^{41}\) As of mid-2015, however, the government has opened a dedicated web site\(^{42}\) that offers data and information voluntarily made available by local and central administrations. Such data, while valuable for scholarly research, are still a far cry from constituting an Italian FOIA.

### Violations of User Rights

Violations against user rights are uncommon in Italy. Criminal defamation laws remain a grave threat to online journalists and social media users, particularly in the ambiguous form they have been applied to the online sphere. A new antiterrorism law was passed in April 2015 extended the period ISPs must keep users’ metadata from 12 to 24 months, despite a ruling from Europe’s high court striking down such requirements as an affront to human rights.

### Legal Environment

As a signatory to the European Convention on Human Rights and other relevant international treaties, freedoms of speech and the press, as well as the confidentiality of correspondence, are constitutionally guaranteed in Italy.\(^{43}\) Yet, given the country’s civil law system, inconsistent judicial interpretations are not unusual. This has created some uncertainty when judges issue conflicting decisions on similar cases related to internet freedom, such as intermediary liability. For this reason, online free expression advocates have focused their efforts on proposing legal amendments to improve protections and prevent censorship rather than engaging in public interest litigation.\(^{44}\)

An inter-parliamentary committee appointed in July 2014 to draft an internet bill of rights released its nonbinding “Declaration of Internet Rights” in July 2015. The declaration makes Italy the first European country to release such a document, following in the footsteps of Brazil.\(^{45}\) The declaration contains language defending the right to internet access, data protection, net neutrality, anonymity,

---

39 The first candidate was Milena Gaibanelli, a journalist, who declined then followed by Stefano Rodotà, former leader of the Privacy authority. In the end the incumbent president, Giorgio Napolitano, was re-elected.
40 Grillo was criticized on his blog for the advertisements revenues from his blog. See Il Blog di Beppe Grillo, [http://www.beppegrillo.it/](http://www.beppegrillo.it/).
44 Andrea Monti (lawyer specialized on Internet freedom and activist), in a conversation with author, February 20, 2012.
and the right to be forgotten. Some observers criticized the declaration for falling short in protecting free speech, balancing copyright, and protecting anonymity and encryption.

Several laws present a threat to internet freedom in the country. Italy passed a new antiterrorism law in April 2015 that broadened language in the criminal code on terrorist recruitment as well as the endorsement or incitement of terrorism to include their action via online channels. Critics worry that the law will be applied broadly and may sanction legitimate instances of free expression that fall within international norms for protected speech. On a positive note, the government withdrew provisions from the bill that would have authorized law enforcement agencies to remotely break into private computers. Prime Minister Renzi noted that the delicate issue needed further discussion.

Defamation is a criminal offense in Italy, punishable by prison terms ranging from six months to three years and a minimum fine of EUR 516 (US$670). In cases of libel through the press, television, or other public means, there is no prescribed maximum fine. Though these provisions are rarely applied, civil libel suits against journalists, including by public officials and politicians, are a common occurrence, and the financial burden of lengthy legal proceedings may have chilling effects on journalists and their editors. As of May 2015, there have been extremely few libel suits against bloggers and other online writers in Italy.

**Prosecutions and Detentions for Online Activities**

No online activists have been detained, prosecuted or sanctioned by law enforcement agencies for disseminating or accessing information on the internet. However, concerns remain over the enforcement of libel law on platforms such as Facebook. In early 2013, a young woman who posted negative and racist remarks about her former employer on the social network was found guilty of libel and made to pay a EUR 1,000 (US$1,100) fine. The prosecution successfully argued that libel may occur through any medium, online or traditional, that can reach a larger public. Going further, the third-level appeals court convicted a non-commissioned officer of the GdF who posted negative comments against a colleague on Facebook, even though the culprit never mentioned the colleague's name. The court ruling reported that it is sufficient that enough details are included so that the offended person can be identified by as few as two persons. It was later struck down on appeal.

---


48 Sghirinzetti, “Italy: Anti-terrorism decree to strengthen government surveillance.”


Surveillance, Privacy, and Anonymity

Monitoring of personal communications is permissible only if a judicial warrant has been issued, and widespread technical surveillance is not a concern in Italy. Wiretapping is generally restricted to cases involving ongoing legal proceedings, except for terrorism investigations. In such instances, since 2001, “pre-emptive wiretapping” may occur even if no formal prosecutorial investigation has been initiated. More lenient procedures are also in place for Mafia-related investigations.53 Overall perception is that the country’s authorities are engaged in a large number of wiretaps,54 but that is probably an exaggeration. On the other hand, the news media regularly publicize wiretap information that is leaked to them and have generally avoided facing jail sentences or even high fines for disseminating classified information.

In March 2008, Parliament approved a law (No. 48 of 2008) that ratified the Council of Europe’s Convention on Cybercrime, which established how long internet-related communication data should be retained.55 This matter was further refined with the inclusion in the Italian legislative system of the 2006 EU Data Retention Directive.56 Although the Court of Justice of the European Union struck down the directive in 2014, Italy passed an antiterrorism law in April 2015 that extended the period ISPs must keep users’ traffic records (metadata), as opposed to the content of communications—from 12 to 24 months.57

Providers must retain information such as broadband internet data, internet telephony, internet use via mobile phone, and email activity. The records can only be disclosed in response to a request from a public prosecutor (a judge) or a defendant’s lawyer, and, like their counterparts elsewhere in Europe, Italy’s law enforcement agencies may ask ISPs to make such information readily available so that they can respond to the needs of criminal investigations. Given the technical burden of this directive, most ISPs now use a third-party service that offers the necessary security guarantees for encryption and data storage. Finally, the law extends the period that internet providers must retain user data to 24 months.

As Italy moves towards greater e-governance, some concerns have been raised over the protection of user data in the hands of public agencies. In the past, the national postal service Poste Italiane’s certified electronic mail (PEC) service was named as the public agency most damaging to individual privacy at the “Annual Big Brother Awards,” an event hosted by civil society activists for greater privacy, for its gross mishandling of private information kept by the government’s Registro delle Opposizioni, a register of people who wish to keep their contact information hidden from advertisement companies.58 Nevertheless, it is now mandatory for all business to use the PEC service in their communications with the public administration to cut costs and reduce paperwork.

---

54 Although it is difficult to determine the real number of people affected by wiretaps (estimates range from 25,000 to over 130,000), many individuals who are caught up in wiretaps have no incriminating connection to the main target of the eavesdropping. The current law stipulates that such peripheral communications cannot be transcribed and any recordings should be destroyed right away, though this is not always carried out in practice. Thus it may happen that some exchanges are recorded and leaked to the media. This is the problem that the proposed bill on electronic surveillance was meant to address.
57 Sghirinzetti, “Italy: Anti-terrorism decree to strengthen government surveillance.”
Finally, in June 2015, the Privacy Authority published the long-awaited new guidelines for managing browser cookies. These guidelines signal an improvement from those published in 2012 that some found cumbersome to implement.59 Earlier in the year, the authority also launched a public consultation to define guidelines and rules for the “Internet of Things.”60

Intimidation and Violence

Reports of extrajudicial intimidation or physical violence in response to online activity are rare, although individuals directly exposing the activities of organized crime in some parts of the country may be at risk of reprisals.

Technical Attacks

The most common forms of technical attacks in Italy are the defacement or launching of denial-of-service (DoS) attacks against websites—mostly government-linked ones—as a form of political protest.61 More serious cyberattacks—particularly against banks, government institutions, and business websites—remain a problem in Italy, as in other European Union member states. Nevertheless, Italy does not rank highly on the list of countries identified as points of origin for cybercrimes.62

The law enforcement agency with primary responsibility for cybercrimes is the Postal and Communications Police Service. Police officers are primarily concerned with cybercrime in the form of child pornography, cyber-bullying, and various forms of fraud.63 In May 2013, the Italian Ministry of Interior was attacked by the Italian branch of Anonymous in retaliation for the arrest of a group of “hack-tivists” a few days earlier.64 The country’s official cybersecurity strategy was published in December 2013.65

In July 2015, the Milan-based private security firm Hacking Team was hacked, leading to the release of several hundred gigabytes of emails and other data that was later posted to Wikileaks.66 The company provides software applications to intelligence agencies around the world and had been criticized in the past for cooperating with nondemocratic regimes and lacking sufficient consider-

62 An independent report by HostExploit shows Italy scoring quite well on a “badness” scale (France, Germany and the United Kingdom, all get a worse score). These results are graphically visible in here: Global Security Map, “Italy,” accessed 19 May 2015, http://globalsecuritymap.com/#it.
63 Figures on cybercrime are difficult to assess, as the main providers of data are computer security companies such as Symantec or government entities like the postal police, as opposed to “third-party” sources. Nevertheless, Italy’s rates appear to be slightly above the world average. See, Tiziana Moriconi, “Crimini online, i dati italiani,” [Online Crime, the Italian Data] Daily Wired, November 23, 2010, http://bit.ly/1G9KQk1; Alessandra Talarico, “Cybercrime. Italia vittima e carnefice: è il paese che più abbozza al phishing e tra i più attivi negli attacchi web based,” [Cybercrime. Italy Victim and Victimizer: It Is the Country That Takes the Bait in Phishing and Is Among the Most Active in Web-Based Attacks] Key4Biz, April 22, 2010, http://bit.ly/1GEzXBD.
Italy

ations of users' privacy. The company has been classified by the nongovernmental organization Reporters Without Borders as an "Enemy of the Internet."


Key Developments: June 2014 – May 2015

- Courts upheld users’ “right to be forgotten” in Japan, requiring search engine companies to delete links to material at the user’s request in specific cases (see Content Removal).

- Despite privacy concerns, the rollout of the “My Number” national resident registry system is scheduled for late 2015 and early 2016 (see Surveillance, Privacy, and Anonymity).

- Telecommunications companies eased restrictions on third-party SIM cards that observers feared had been limiting users’ ability to switch carriers (see ICT Market).
Introduction

As in past years, privacy concerns, data leaks, and cyberattacks were key issues for Japanese internet users during the coverage period. Japan’s constitution protects all forms of speech and prohibits censorship, while the government, especially the Ministry of Internal Affairs and Communications, maintains a hands-off approach to online content, which is generally regulated voluntarily by industry players. Internet penetration is over 90 percent. Despite strong access, however, some legislation disproportionately penalizes specific online activities.

As part of the Abe administration’s strategy to boost national security, lawmakers passed the Act on the Protection of Specially Designated Secrets in 2013. The legislation, which criminalized both leaking and publishing broadly defined national secrets regardless of intent or content, has repercussions for journalists, whistleblowers, and civil society watchdogs, particularly in the age of the internet. In a review of Japan’s human rights practices in July 2014, the United Nations Human Rights Committee said the legislation laid out “a vague and broad definition of the matters that can be classified as secret” and “high criminal penalties that could generate a chilling effect on the activities of journalists and human rights defenders.”

Attention to data security also escalated in 2014, with the high-profile arrest and trial of an engineer for leaking personal data belonging to customers of the Benesse educational services corporation. In Japan’s largest data leak to date, Benesse confirmed “the leak of personal data of at least 7.6 million people [noting that]…the problem could ultimately affect more than 20 million.”

Such attention to security measures is of particular concern for national and local governments as they gear up for the introduction of the “My Number” system of personal ID numbers throughout the country. Amendments to the Act on the Protection of Personal Information to strengthen data privacy penalties to remove personal information that identifies individuals were passed in the Diet in early September 2015. Such amendments may also forestall fears of possible data leakages with the rollout of the “My Number” system in October 2015.

---

"マイナンバー法改正案が衆院可決 貯金口座にも適用 "[My Number Law proposal enters committee, Lower House plenary session] Nikkei Asian Review, April 23, 2015, http://s.nikkei.com/1L1MX8;
Obstacles to Access

In general, Japanese internet users experience few obstacles to access. Internet access remains high, and mobile phone companies are increasing reaching out through expanded technological offerings. One major development in the past year has been the availability of third-party SIM cards with mobile operators unlocking phones for a small fee, and the greater availability of SIM-free models of phones and tablets.

Availability and Ease of Access

Internet penetration was at 91 percent in 2014, up from 90 in 2013. Mobile phone penetration reached 120 percent in 2014. Official statistics report slightly over 155 million mobile phones (including personal handy-phone systems, or PHS) in use in Japan as of March 31, 2015, equivalent to a penetration rate of 121.1 percent and demonstrating an increase of 4.9 percent over the previous year’s figure. Access is high quality with competitive speeds averaging 15.2 Mbps in early 2015.

The average cost of internet access is around JPY 5,000 (US$50) per month, though many providers bundle digital media subscriptions, Voice over IP (VoIP), and email addresses, pushing expenses higher. While this remains within reach of most, declining average incomes make staying connected increasingly costly, especially for the younger generation. According to data published in 2013, the average household in Japan spends around JPY 6,925 (US$69) for mobile service per month, or JPY 83,099 yen (US$830) per year. The private Wire & Wireless service offers free Wi-Fi access in restaurants, coffee shops, and some train stations; registration requires an email address.

As these figures suggest, access is well distributed across the population, though less common among the elderly. According to the MIC Information Communications Statistics Database, internet penetration was 72 percent for children aged 6 to 12, and over 95 percent in the age ranges of 13 to 49, compared to 21 percent for people over 80 years of age. Mobile phone operators are expanding their market for handsets designed for children and for the elderly, with easy-to-use, large-button phones.

Restrictions on Connectivity

There are few infrastructural limitations on internet access in Japan, though the vulnerability of

---

10 Informal Freedom House survey of providers’ costs.
11 The average monthly income for working households in 2010 was 700 yen (US$7) less than it was in 1990. See, Ministry of Internal Affairs and Communications Statistics Bureau, “Average Monthly Income and Expenditure per Household (Workers) 1955-2010,” http://www.stat.go.jp/data/chouki/zuhyou/20-06.xls.
Japan

Japan's communication network became apparent in 2011, when an earthquake and tsunami hit Japan's east coast, triggering a nuclear plant accident. Infrastructure was severely damaged, leaving many people without service for periods from a few days to one month and restricting relief efforts. Mobile phone usage dropped by almost half in the affected areas.\(^{15}\)

Network congestion and server outages—the result of increasing smartphone traffic due in part to many applications sending automatic signals every minute—also frequently affect mobile use. KDDI, one of three major mobile carriers, reported large scale disruptions in 2012 and 2013. Fewer disturbances were reported during this year’s coverage period.

In 2013, Nippon Telegraph and Telephone Corporation's (NTT) Docomo announced an expansion in LTE base stations to augment its Xi LTE and FOMA 3G services.\(^{16}\) Providers such as Asahi-net offer WiMAX plans with mobile routers capable of accessing multiple networks throughout the country.\(^{17}\) Historically, Japan’s internet connections were forged through cooperation among government agencies (including ministries and NTT, which was a government-owned monopoly until 1985), higher education institutions (mainly national universities), and national research institutions. According to the internet timeline available on the Japan Network Information Center website, the first network operations (known as the “N-1 Network,” in operation from October 1974 to December 31, 1999) were a joint undertaking initially operated by the University of Tokyo, the University of Kyoto, and NTT that later expanded to link other national universities in Japan.\(^{18}\) The network of connected institutions started to expand in the mid-1980s with the start of JUNET (Japan University Network), pioneered by Keio University professor Jun Murai. The first Japanese university to connect to an overseas university was the Tokyo University of Science (connecting with the City University of New York) in 1985.

ICT Market

Japan has three major mobile operators—KDDI Au, NTT Docomo, and Softbank. All use the CDMA wireless network or a variant. NTT, formerly a state monopoly, was privatized in 1985 and reorganized in 1999 under a law promoting functional separation between the company’s mobile, fixed-line, and internet services.\(^{19}\) Asymmetric regulation, which creates stricter rules for carriers with a higher market share, helped diversify the industry.\(^{20}\) While the telecommunications market operates with hundreds of providers offering FTTH, DSL, CATV, FWA, and BWA services, the NTT group remains dominant in practice.\(^{21}\) NTT Docomo held close to 40 percent of Japan’s mobile market in 2015.\(^{22}\) No major foreign operators have successfully penetrated the telecommunications market independently; smartphone devices manufactured by Apple and Samsung are available to consum-


ers through partnerships with the major mobile operators. Consolidation in the mobile industry continued in Japan during this year’s coverage period, as Ymobile, which was formed in August 2014 through a merger of Emobile (formerly a roaming mobile company) and Willcomm (a PHS carrier),23 joined the Softbank group of companies as of April 1, 2015.24

Despite this background, increasing smartphone use has made the mobile market more competitive and resulted in improved pricing options: bundling mobile tablet plans with subsidies for second and third devices purchased by consumers; decreases in prices for data and family plans; and the introduction of benefits for long-term customers, such as those offered by Docomo to customers with 5- to 15- year histories of continuous service.

In a positive development, third-party SIM card availability increased during the coverage period. In the summer of 2014, the government announced plans to require cellphone carriers to unlock the SIM cards in mobile phones if requested by users, facilitating the use of third-party prepaid SIM cards.25 In October 2014, the MIC issued new guidelines concerning SIM card unlocking.26 The new guidelines, which went into effect in May 2015, also stipulate that users must pay outstanding handset costs prior to switching carriers. Though the guidelines were still subject to criticism,27 they helped address concerns that the cost of switching providers favored the dominant players and created a barrier for new entrants to the market. Besides benefitting Japanese consumers,28 the change will serve the influx of tourists to Japan anticipated prior to the 2020 Tokyo Olympics.29

Regulatory Bodies

There is no independent regulatory commission in Japan, though observers believe that the industry has generally improved since the 2001 establishment of the Ministry of Internal Affairs and Communications (MIC), comprised of two former ministries (the Ministry of Home Affairs and the Ministry of Posts and Telecommunications) which were merged with the central government’s Management and Coordination Agency. This “super ministry” regulates the telecommunications, internet, and broadcast sectors.30 Nongovernmental, nonprofit organizations supported by the relevant companies in the sector have been formed to self-regulate the industry. These include television’s Broadcasting Ethics & Program Improvement Organization, the Content Evaluation and Monitoring Association for mobile platforms, and the internet’s Content Safety Association, which manages blocking of child pornography online.31

---


26 “New rule to OK unconditional switching of mobile carriers,” Japan Times, October 1, 2014.


28 “Phone users in Japan still paying for plenty of stuff they don’t need,” Japan Times, May 23, 2015.

29 “Narita airport to get SIM card vending machines,” Japan Times, July 17, 2015.

30 Before 2001, regulation was managed by the now-defunct Ministry of Post and Telecommunications, before that, the Diet.

Japan

Limits on Content

Politicians embraced social media for campaign purposes during the 2013 Upper House election after outdated restrictions on digital electioneering were revised during the previous coverage period and continued to expand online campaigning in the December 2014 general election to the Lower House. Activists and civil society also used digital tools to promote local civic causes, and online activity was increasingly effective as a means to combat hate speech and racism.

Blocking and Filtering

No direct political censorship has been documented in Japan. ISPs voluntarily filter child pornography, and many offer parents the option to filter other immoral content to protect young internet users. Depictions of genitalia are pixelated to obscure them for internet users based on a common—though poorly-articulated—interpretation of Article 175 of the penal code, which governs obscenity. Otherwise, individuals or police instruct ISPs to administratively delete contested or illegal content.

The threat of official content restrictions looms periodically during public debates about child safety, though carriers and content producers have successfully resisted intrusive regulation. In 2007, the MIC ordered mobile operators to install filtering software enabling parents to control content seen by their children. A coalition of groups, including the Japan Internet Providers Association and the user rights organization Movement of Internet Active Users lobbied against the mandate and mobile users can now select voluntary filters. Complaints to the official Consumer Affairs Agency about quasi-gambling functions in games played by children on mobile devices shot up in 2011, along with calls for government regulation. Instead, in 2012, game developers Gree and DeNA Mobage voluntarily adopted caps on purchases of virtual items by minors. Games integrated with social networks have also been criticized for their potential for abuse by sexual predators.

Private interests also pressure ISPs to restrict content. In 2012, a coalition of music rights advocates were reportedly offering to sell service providers a tool to detect whether material being uploaded to the internet is subject to copyright, and sever connections of users violating Japan’s strict copyright laws. No follow-up was reported.

Content Removal

Throughout the coverage period, there were a number of cases in Japan involving the “right to be forgotten,” a practice allowing users to request that search engines delink material about them from

Japan

public results in their country. In October 2014, the Tokyo District Court handed down a provisional order requesting that Google delete half of 237 entries involving a plaintiff’s name and subsequently entered text. This incident was noted as possibly the first instance in Japan involving the courts and the removal of search results, and Google Japan stated its willingness to comply with “legal take-down notices.” Attention to this issue grew in the following weeks, and in November 2014, Yahoo Japan created an expert panel to investigate the right to be forgotten, with a six-month mandate to examine the situation. At the time, Yahoo Japan also noted that it does not comply with “requests to remove search results except for certain cases involving past crimes,” citing the reason that “one company alone cannot decide what society should and should not have access to.”

In March 2015, Yahoo Japan unveiled a new set of rules, stating that “it will respond to requests to remove information from search results after weighing privacy protection versus freedom of expression and the right to know...including information such as individuals’ personal addresses and telephone numbers.” It should be noted that contrary to the EU’s sweeping laws concerning the right to be forgotten on the internet, to date there is no similarly broad law in Japan, and cases against search engine companies have been dealt with on an individual basis by each search engine company separately.

The 2001 Provider Liability Limitation Act directed ISPs to establish a self-regulatory framework to govern takedown requests involving illegal or objectionable content, defamation, privacy violations and copyright infringement. In 2002, industry associations produced guidelines designed to protect ISPs from legal liability within the jurisdiction of the Japanese courts. Under the guidelines, anyone can report material that infringes directly on their personal rights to the service provider, either to have it removed or to find out who posted it. No third party can do so. The provider notifies the individual who posted the content, and either fulfills the request with their permission or removes the content without the authors’ approval if they fail to respond. If the poster refuses permission, the service provider is authorized to assess the complaint for themselves, and comply if they believe it is legitimate. In this scenario, an ISP could give the complainant information to identify the poster—such as their name or IP address—without that person’s consent, leading to privacy concerns. This process is voluntary, but by complying, service providers protect themselves from civil liability.

In recent years, content removals have focused on obscene content, including child pornography and “revenge porn,” explicit images shared without consent of the subject. After complying with a takedown order in August 2014, Facebook was further ordered by a Tokyo court in October 2014 to “disclose the IP addresses used by fake accounts that were posting revenge porn.” A law to address online harassment by means of posting explicit images without the subject’s consent passed in November 2014. Prior to this law’s passage, upon receiving a complaint, providers were legally obligated to contact the original poster of the images to indicate that such objectionable content would be taken down within seven days. In the case where there was no response from the original poster, the

40 “Yahoo Japan to set up expert panel on ‘right to be forgotten,’” Mainichi Daily News, November 8, 2014.
45 “Court orders Facebook to reveal revenge porn IP addresses,” Japan Today, October 22, 2014.
content could be legally deleted by the provider. The new law passed in 2014 reduced the duration of time allowed to the providers to comply with takedown requests from seven days to two days (see Legal Environment).\footnote{“Ribenjiporuno ni chōeki 3 nen ika no bassoku jimin hōan teishutsu e” (“LDP submit Bill to punish revenue porn with up to three years’ imprisonment”), Nihon Keizai Shimbun, October 12, 2014. (http://www.nikkei.com/article/DGXLASFS11H03_S4A011C1PE8000/)}

Between November 27 and December 31, 2014, over 100 complaints of revenge porn were received by the National Policy Agency.\footnote{Takuro Yagi, “Police field 110 complaints of ‘revenge porn’ in first month of tough new law,” Asahi Shimbun, April 3, 2015.}

The Internet Hotline Center, operated through the Internet Association Japan as part of a contract with the National Police Agency, cooperates with ISPs to solicit reports of illegal or harmful content from the public.\footnote{Internet Hotline Center Japan, “Annual Statistics 2013;” May 1, 2014, http://www.internethotline.jp/statistics/2013e.pdf.} While the center received a record high of 196,474 calls in 2012, 150,352 reports were received in 2014.\footnote{Internet Hotline Center Japan, “Annual Statistics 2014,” [in Japanese] http://www.internethotline.jp/statistics/2014e.pdf.} (Over 40,000 reports were received in the first three months of 2015.)\footnote{Internet Hotline Center Japan, “Statistical Information,” [in Japanese] 2007-2014, http://www.internethotline.jp/statistics/.} The center’s breakdown of reports by type reveals 23 percent involved illegal information (information involving illegal activities such as public displays of obscene materials or “publicly inciting or soliciting others to abuse controlled substances”) with over 50 percent originating from overseas; 3 percent involved harmful information (information that could invite illegal conduct, related to suicide, or which is “difficult to judge as illegal but seems to be illegal”) with 67.5 percent of the cases originating overseas; and 75 percent which “were beyond scope of its operational guidelines, including defamation, slander, murder notices, intellectual property infringement, information inappropriate for children, and other cases.”\footnote{Internet Hotline Center Japan, “Annual Statistics 2014.”} Providers may, but are not obliged to, comply with content removal requests submitted through the center.

### Media, Diversity, and Content Manipulation

Japanese citizens exercise some self-censorship online, often on historical and social issues. The society at large prefers “harmony,” and people avoid criticizing the role of Japan’s Emperor, especially when connected with historic issues like World War Two. Individuals and public figures who break this code risk censure and even attacks from right-wing fanatics, who notoriously tried to assassinate the Nagasaki mayor on these grounds in the 1990s. Though exceptional, incidents like this still exert a chilling effect on Japanese expression.

There are few known cases of the government or powerful groups proactively manipulating online news or other content. In a significant exception, officials and the Tokyo Electric Power Company withheld data about pollution after a nuclear power plant in Fukushima prefecture was severely damaged by the 2011 earthquake and tsunami, and citizens unwittingly exposed themselves to radiation. The MIC requested that four industry associations monitor false or unsubstantiated content circulating about the disaster online, including on social networks. Some observers said this was a measure to control public discourse, though deletions were not widespread. Service providers removed content, which included images of corpses, in at least 13 cases,\footnote{Madeline Earp, “Freelance, online reporting discouraged on nuclear threat,” Committee to Protect Journalists (blog), April 14, 2011, https://cpj.org/x/42f5; Ministry of Internal Affairs and Communications, “Demand for Telecommunications Carriers Associations Regarding the Appropriate Response to False Rumors on the Internet Related to the Great East Japan Earthquake,”[in Japanese] press release, April 6, 2011, http://bit.ly/1PjW9lt.} though the National Police...
Japan

Agency reported 41 items for review.\(^5\) Others found an outlet to report on the aftermath of the disaster online.\(^4\)

In 2014, media observers expressed concern that the government had enjoyed undue influence over mass media content when the *Asahi Shimbun* newspaper retracted stories about the “comfort women” forced to work in army brothels during World War Two. The stories, which the paper said relied on one misleading source, had provided support to a revisionist effort to refute women’s assertions they were kidnapped and assaulted by Japanese soldiers. Since this position is held by many Abe supporters, readers speculated the inaccurate reports were the product of official “guidance.”\(^5\) However, there was no evidence of a direct link between the coverage and Abe’s administration, or of political “guidance” influencing online content.

During the 2013-14 coverage period, some news reports expressed concern about nationalistic discourse by Japanese web trolls, or *netōyo*, escalating into hate speech online, particularly targeting South Koreans and Chinese communities amid territorial disputes between Japan and their respective governments.\(^6\) Tensions were high during 2013. In one incident, an advertisement with a government seal that appeared to support revisionist history was widely circulated on social media, though it turned out to be a fake.\(^7\) Nationalist discourse and incitements to violence directed at South Korean and Chinese people also flourished on the internet.\(^8\) However, during the coverage period, a movement to combat hate speech gained ground (see Digital Activism).

Blogs have a significant impact on public opinion, and several independent journalists are becoming influential through personal or commercial websites and social media accounts. Yet most online media remain small and community-based,\(^9\) with no major national successes, and the mainstream media’s habit of compliance and restraint may be standing in the way of the combative online news culture flourishing elsewhere in Asia.\(^6\) Kisha clubs, formal organizations only open to traditional media companies, and an advertising market that favors established players may be preventing digital media from gaining a foothold in the market. Kisha clubs provide essential access to officials in Japan, but have been accused of discriminating against new media practitioners in the past. In 2012, at least one online journalist was denied access to one of their Tokyo locations,\(^6\) and the only two freelancers permitted to join an official group of 40 reporters on a tour of the nuclear disaster site were forbidden from taking equipment.\(^6\) Some online news outlets have struggled to sustain themselves financially. *OhmyNews*, a South Korean platform, established a Japanese operation in 2006, but

Japan


YouTube, Twitter, Facebook, and international blog-hosting services are freely available, as are popular domestic platforms like Niconico Dōga, a video-sharing site, and LINE, a Korea-based chat application that was launched in Japan in 2011.

Digital Activism

To date, much digital activism has been effective at the local rather than national level, including maps sharing public information about disaster relief,64 or tracking racist graffiti in Tokyo. During the coverage period, anti-hate speech advocates using the internet to draw attention to and combat online slurs saw progress in a number of initiatives. In early 2015, a group of Korean residents and Japanese supporters established the Antiracism Information Center, which has a website and a physical location in Tokyo, to counteract hate speech online.66 In May 2015, the Japanese video streaming website Niconico Dōga reported that it “shut down the official channel of the anti-Korean activist group Zaitokukai, citing violations of [its] terms of service.”67 Politicians also responded. In September 2014, the Kunitachi city assembly “adopted a statement demanding the central government take legislative action to ban ‘hate speech’ rallies.”68 Separately, in December 2014, a Japanese internet activist and academic erected a whistleblower website to challenge the state secrets law.69

Violations of User Rights

During the 2014-15 coverage period, two important pieces of legislation passed into law that may have implications for digital freedom of expression. After passage in the Lower House, the state secrets law, which some fear could threaten free expression, underwent several refinements before coming into force in December 2014. However, these revisions failed to address criticisms about the potential penalties attached to revealing information in the public interest. Separately, a law criminalizing revenge porn and other forms of online harassment passed in November 2014.

Legal Environment

Article 21 of Japan’s constitution prohibits censorship and protects freedom of “speech, press and all other forms of expression,” as well as the “secrecy of any means of communication.”70 In general, individuals and media can exercise this in practice, though social and legal constraints exist.

The Act on the Protection of Specially Designated Secrets came into force in December 2014 after

---

passing in 2013, despite objections from the opposition, civil society, and protesters. The law gives a range of officials the discretion to indefinitely restrict public information pertaining to national security in any one of the categories of defense, foreign affairs, “prevention of designated harmful activities” (such as “counter-intelligence”), and prevention of terrorism.71 Overseen by government officials rather than an independent body, it offers no protection for whistleblowers who reveal wrongdoing, leaving it open to misuse against Wikileaks-style whistleblowers and journalists.72 For those people who handle such state-designated secrets, intentional leaks are punishable by up to 10 years’ imprisonment, and unintentional leaks by up to 2 years. Individuals who knowingly receive such secrets from an administrative organ for the sake of the public interest risk up to 5 years for intentional disclosures and 1 year for disclosures via negligence.73

Refinements to the law during the coverage period outlined four main fields (defense, diplomacy, anti-espionage, and antiterrorism measures) in which 55 categories of state secrets can be applied.74 Responding to criticism,75 the government solicited public comments for a period of 30 days in July and August 2014.76 After receiving more than 20,000 public comments,77 draft revisions were tabled. Yet even these drew concerns, particularly in terms of how the law would actually work in practice.78 In October 2014, protests continued throughout the country prior to the bill’s coming into force in December.

Other laws include potentially disproportionate penalties for online activity, including a 2012 legal revision targeting copyright violators—including any internet user downloading content they know has been illegally copied, as opposed to just those engaged in piracy for commercial gain.79 While both uploading and downloading pirated material was already illegal under the copyright law, with uploaders subject to 10 years’ imprisonment or fines up to JPY 10 million (US$102,000), the version in effect since October 1, 2012 added two years in jail or fines up to JPY two million (US$20,500) for downloading a single pirated file.80 The Japanese Bar Association said that downloading, as an essentially insignificant personal act, should be regulated by civil instead of criminal laws.81

A 2013 revision of the Public Offices Election Act undid long-standing restrictions on use of the internet for election campaigns. Limits remain on paid online advertising and campaign emails, which could only be sent directly by a party or candidate—not a supporter—in a measure designed to prevent fraud, though members of the electorate can freely solicit support on social media.82 While these provisions were contested and revisions are still planned,83 news reports said politicians vio-
Japan

In June 2014, a law passed punishing possession of images of child sexual abuse, with a possible penalty of one year imprisonment. In January 2015, police raided Amazon Japan’s head office and affiliated distribution center after complaints the website was facilitating the sale of illegal material depicting children. The company said it was cooperating.

Heightened awareness of revenge porn and online harassment culminated in the ruling Liberal Democratic Party (LDP) passing a bill criminalizing revenge porn in November 2014. The law stipulates that “offenders who distribute such images could face up to three years in prison or a fine of up to JPY 500,000 yen ($5,100), with third-party distribution also leading to up to one year in prison or a fine of JPY 300,000 yen ($3,060).”

In August 2014 the UN Committee on the Elimination of Racial Discrimination advised the Japanese government to enact laws to address hate speech, including statements made on the internet and offline. A national bill has yet to be drafted.

Prosecutions and Detentions for Online Activities

While no citizens faced politically-motivated arrest or prosecution for content they have published online, in May 2015, police arrested a 43-year-old Tokyo resident for posting an online threat in the 2channel bulletin board against Princess Kako, a member of the Japanese royal family. In February 2015, news reports said 40 people were arrested for illegally uploading copyrighted material. No disproportionate sentences were reported.

Surveillance, Privacy, and Anonymity

Japan’s Supreme Court protects privacy through its interpretation of Article 13 of the constitution,
Japan

which provides for the right to life and liberty.93 “Secrecy of communication” is also protected under telecommunications laws,94 though some digital activities require registration. Major mobile carriers require customers to present identification documents in order to subscribe, while prepaid SIM cards are not widely available. Internet cafe users are required to produce formal ID such as a driver’s license and register their name and address. Police can request these details, along with usage logs, if they detect illegal online activity.

Under voluntary guidelines drafted by four ISPs in 2005, service providers automatically inform police of internet users identified on pro-suicide websites, and comply with law enforcement requests for information related to acts of self-harm.95 A law enacted in 2003 and revised in 2008 prohibits electronic communications encouraging sexual activity with minors.96 Under the law, all online dating services must register with the police, verify their customers’ ages with a driver’s license or credit card, and delete or block content that appears to involve someone under 18; most services voluntarily monitor messages in real time to ensure compliance.

Under a wiretap law enacted in 1999, law enforcement agents may seek a court order to conduct electronic surveillance in criminal investigations involving drugs, firearms, human trafficking, or organized murders, an exception to articles of other laws that explicitly forbid wiretapping.97 The law obliges agents to notify targets of wiretaps after investigations are concluded and inform the Diet about the number they implement annually. While the law was extremely controversial when it passed, in part due to the authorities’ politicized abuse of surveillance in the past,98 lawmakers were seeking to expand it in December 2012.99 Critics say the law does not prevent the systematic storage of intercepted communications or protect innocent parties.100 Security agents and the military have been accused of implementing surveillance in cases involving national security.101

A law to protect personal information dating from 2003 protects individuals’ data collected electronically by private and public sector organizations, where the data involves more than 5,000 records.102 Law enforcement requests for this data should be supported by a warrant.103 In mid-2014, local news reported that 115 supermarkets and convenience stores in the Tokyo area had contracted with a Nagoya-based software firm to automatically record images of shoplifters and unreasonable customers to share in a network for other stores to blacklist.104 While the businesses cited security measures,
Japan

critics said sharing biometric data without consent conflicts with Japan’s personal privacy law, Act on the Protection of Personal Information, No. 57 of 2003, which includes facial images within its definition of personal information. Amendments to the personal privacy law passed in September 2015, outside the coverage period of this report.

A “My Number” law proposed by the cabinet in 2012 passed the Diet on May 24, 2013.105 Under this system each resident (including non-Japanese residents) will be assigned a unique ID number from October 2015.106 Starting from January 2016, this number, which appears on a photo-ID card containing an electronic data chip, will be used for unified social-welfare services, including taxes, pensions, and healthcare.

The “My Number” system is the most recent in a series of attempts to nationally unify Japan’s Basic Resident Registry procedures. The first was made in 2002 with the introduction of the Resident Basic Register Network System (known as RRNS or “Juki Net”), which was established to facilitate sharing information among local governments in the case of residents who move, register births and deaths, and apply for social services.107 Even upon its introduction, the issue of a nationally available registry service was contested based on privacy issues, with some local municipalities choosing to opt out of the system (such as Tokyo’s Suginami Ward and Yamatsuri town in Fukushima prefecture).108 However, in response to a suit filed by 12 individuals in Aichi prefecture, the Supreme Court ruled in 2008 that Juki Net was constitutional and all citizens were subject to mandatory enrollment.109

Politicians and bureaucrats said personal identification numbers would streamline social benefits and maintain accuracy and fairness in the provision of government services,110 as well as assist in identifying individuals in the case of natural disasters.111 However, it remains unclear how the data would be stored in order to provide services offered through multiple levels of government.112 The Japan Federation Bar Association in 2012 highlighted the system’s possible privacy issues when the bill was first introduced.113 In May 2013, the Japan Medical Association also contested the new system based on security issues involving medical records.114 Others said its planned expansion into other government-related services, including potential use by the private sector, could also facilitate fraudulent use of personal data.115

Concerns about the implications of “My Number” for data privacy and security increased in 2014 with the arrest and subsequent trial of an engineer employed by a subsidiary data management company affiliated with the corporate group Benesse. He was charged with facilitating the country’s largest personal data leak on record for the educational services company. Benesse “confirmed the leak of personal data of at least 7.6 million people [noting that]...the problem could ultimately affect

---

109 Bowe, “In Japan, National ID Proposal Spurs Privacy Concerns.”
110 “EDITORIAL: ID number system should be a tool to build a fair society,” The Asahi Shimbun.
112 “’My number’ is dangerous,” The Japan Times.
114 Bowe, “In Japan, National ID Proposal Spurs Privacy Concerns.”
115 “’My number’ is dangerous,” The Japan Times.
more than 20 million.” A public opinion survey conducted by the Cabinet Office in January 2015 found that while only 28 percent of respondents were aware of the “My Number” system, nearly a third were concerned that “My Number” information could be used for unauthorized purposes.

Intimidation and Violence

No physical violence has been reported against bloggers or internet users in relation to their online activity.

Technical Attacks

While distributed denial-of-service (DDoS) attacks were part of the arsenal used by nationalists in Japan, China, and South Korea to target perceived opponents in other countries, and cyberattacks have been reported against commercial and government targets, they are not known to have been used to systematically target individuals or civil society groups. However, 1.25 million citizens were affected when hackers released personal information obtained by illegally accessing Japan’s pension system using an email virus in mid-2015.

Japanese law enforcement agencies are expanding their cybercrime capacity to respond to foreign cyberattacks and domestic data leaks. The National Policy Agency announced a new Cyberattack division in January 2015. In 2013, the Kanagawa and Osaka police departments established separate divisions for addressing cybercrime, adding to police departments in Tokyo and 12 other prefectures. Later that year, the Abe administration added the legislative position of “Chief Information Officer” to the national-level cabinet, and the Information Security Policy Council within the National Information Security Center released a “Cybersecurity Strategy” and an “International Strategy on Cybersecurity Cooperation.”

The central government has become increasingly aware that there is a shortage of data specialists and data engineers within the government ranks. In January 2015, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) was launched, “serving as a base of operations for […] cybersecurity.” In the first few months of operations, the NISC received applications from private-sector programmers with an eye to recruiting up to 10 employees (to be employed “as

116 “1,789 file Y100 mil damages suit against Benesse over data leak,” Japan Today.
119 William Mallard and Linda Sieg, “Japan pension system hacked, 1.25 million cases of personal data leaked,” eds. Robert Birsel and Clarence Fernandez, Reuters, June 1, 2015, http://reut.rs/1QkFniW
government employees for up to five years”), as well as a staff of 100 people.126 Also in the early
months of 2015, the government aimed at recruiting such workers through sponsored events such
as “hackathons.” A “cybersecurity competition” was held in early February 2014 (Security Contest
2014, or SECCON), drawing a total of “4,186 participants of 58 different nationalities” with the final
rounds being held among “90 participants in 24 teams from seven nations and regions.”127 Despite
the increased focus by the central government, it remains to be seen if recruitment measures will
be continued on a permanent basis (which would make them subject to the age restrictions and the
examination system for all national, prefectural, and local civil servants) or if national, prefectural,
and local governments will turn to private-sector information-technology companies as suppliers of
technical staff on an outsourced contract basis.

126 Oliver, “Japan government to recruit ‘white hat’ hackers for landmark cybersecurity initiative.”
ly/1NhJ6JA.
Jordan

Key Developments: June 2014 – May 2015

- The Media Commission continued to block news websites that were operating without a government license as required by the amendments to the Press and Publications Law passed in September 2012. Charges were also pressed against websites operating without a license (see Blocking and Filtering).

- Two licensed news websites, Al-Kawn News and Saraya News, were blocked in December 2014 and January 2015, respectively, for publishing content related to the Jordanian pilot Moath Al-Kasasbeh who fell captive in the hands of Islamic State fighters (see Blocking and Filtering).

- On January 28, 2015, two staff at Saraya News were detained for 40 days and charged by the State Security Court prosecutor under the amended antiterrorism law (see Prosecutions and Detentions for Online Activities).

- Zaki Bani Irshaid, deputy leader of the Muslim Brotherhood in Jordan, was arrested in November 2014 and charged with “harming Jordan’s ties with a friendly state” for a post he published on his Facebook profile criticizing the UAE. On February 14, 2015 he was sentenced to 1.5 years in prison. Two other activists affiliated with the Brotherhood were detained for Facebook comments (see Prosecutions and Detentions for Online Activities).

- On March 11, 2015, the military attorney general asked the prime minister to lift parliamentary immunity from Member of Parliament Tarek Khoury in order to put him on trial for “inciting to undermine the regime.” He had posted comments critical of Jordan’s relationship with Israel on his Facebook page (see Prosecutions and Detentions for Online Activities).
Jordan

Introduction

Internet freedom conditions in Jordan declined over the past year. In April 2014, amendments to the antiterrorism law were passed, broadening the definition of terrorism to include acts that “could threaten the country’s relations to foreign states or expose the country or its citizens to retaliatory acts on them or their money,” an offense that had already been listed in the penal code,\(^1\) which defines terrorism as “any act that can lead to undermining the political regime of the Kingdom.”\(^2\) The new law also explicitly penalizes the use of information and communication technologies (ICTs) to promote, support, or fund terrorist acts. In November 2014, the new antiterrorism amendments were used to sentence the deputy leader of the Muslim Brotherhood, Zaki Bani Irshaid, to 1.5 years of prison with hard labor for “threatening the country’s relation to a foreign state” after he criticized the government of the United Arab Emirates on his personal Facebook page.\(^3\) A number of other activists were arrested and put on trial by the State Security Court for material they published online.

In September 2014, Jordan joined the U.S.-led coalition performing airstrikes against Islamic State (IS) targets in Syria. Opposition groups protested the move using the slogan and hashtag, “Not Our War.” However, after the Jordanian pilot Moath Al-Kasasbeh was taken captive and eventually killed by IS, these expressions of opposition became much less visible. While some say that the killing of the pilot united Jordanians and strengthened sentiments in support of the war,\(^4\) others say dissenting voices decreased due to self-censorship.\(^5\) Meanwhile, government censorship of online content increased after Al-Kasasbeh was taken captive and eventually executed by IS. In December 2014, the State Security Court Prosecutor issued a decree prohibiting the publication of any news items or photos released by IS.\(^6\) Two websites, Al-Kawn News and Saraya News, were blocked for breaking this order. Al-Kawn was unblocked four days later, but Saraya News remained blocked for over a month, while its owner and editor were detained and charged under the antiterrorism law.

Internet access was first provided to Jordanians in 1995, the same year the Telecommunications Regulatory Commission (TRC) was established to regulate the country’s information and communication technology (ICT) sector.\(^7\) Recognizing the economic potential of the internet, authorities actively promoted ICT development in the small kingdom.\(^8\) Once seen as a means for trivial entertainment and the exchange of scandalous or banned information, the internet has grown into a vital instrument for business and an important forum for public discussion. Accordingly, as the number of users began to increase dramatically, the government drew up legal methods for maintaining control over online content and monitoring users, particularly after the regional uprisings of 2011.\(^9\) Constitutional amendments were passed to calm public discontent, improving protections on freedom of expression and strengthening the independence of the judiciary, while parliamentary elections took place.

---

7. The TRC was established as a financially and administratively independent jurisdictional body through the Telecommunications Law No. 13 of 1995 and a subsequent amendment Law No. 8 of 2002.
under a slightly improved electoral framework in January 2013. Most of these however did not materialize into any change in the status quo.

In September 2012, the Press and Publications Law was amended to introduce more restrictions to online media, which was used to block nearly 300 websites in June 2013 for failing to register with the Media Commission. Although most of the sites eventually received licenses and were unblocked, the government continued to block unlicensed news websites over the coverage period. The Universal Periodical Review of Jordan, which took place in October 2013 under the United Nations Human Rights Council, criticized the increased censorship in the country, along with the continued trials of civilians before military courts for offenses related to free speech.10

Obstacles to Access

Mobile broadband has soared in the country, boosted by the introduction of 4G LTE and more affordable pricing. However, competition in the ICT sector is hindered by the influence of Jordan’s existing providers.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), a total of 44 percent of the Jordanian population had access to the internet by the end of 2014, up from 26 percent five years earlier.11 National figures from the Telecommunications Regulation Commission (TRC) estimated the number of users to have increased by end of March 2015 to 76 percent, or 5.9 million users. According to TRC statistics, the number of mobile broadband subscriptions reached 1.5 million by end of March 2015, while fixed-line ADSL subscriptions numbered 218,459. Mobile phone use has also expanded rapidly, and by the end of March 2015, the number of subscriptions was over 11.5 million, representing a penetration rate of 147 percent.12

The expansion of fixed-line internet access has been hampered by the relatively high costs of computers and connectivity. Consequently, fixed broadband subscriptions have decreased since 2009, with only 2.83 subscriptions per 100 inhabitants.13 On the other hand, mobile broadband use has soared to over 1.5 million subscribers.14

For several years, internet connection fees were considered high relative to neighboring countries and the cost of living. Prices have dropped in 2014, but complaints about the quality of service persist. Monthly fixed-line subscription prices currently range from JOD 19.9 (US$28) for speeds of 1 Mbps and an allowance of 10 Gigabytes (GB), to JOD 34.9 (US$59) for speeds of up to 24 Mbps and unlimited download. Orange Jordan also began offering a fiber connection with speeds up to 80 Mbps and unlimited download allowance for JOD 74.9 per month (US$105.5). Postpaid monthly

Jordan

plans for Evolved High-Speed Packet Access (HSPA+) range from JOD 10 (US$14) to JOD 20 (US$28) per month, depending on speeds and data allowances.\textsuperscript{15} By comparison, gross national income per capita is US$4,950, or US$413 per month.\textsuperscript{16} Meanwhile, internet access in many of the country's governorates and remote areas remains poor, as almost all companies concentrate their operations and promotions in major cities, particularly the capital Amman.

Restrictions on Connectivity

There were no restrictions on connectivity seen in Jordan over the past year. However, the centralization of internet backbone infrastructure in government hands remains a concern. The formerly state-owned Jordan Telecom controls the fixed-line network and provides access to all other ISPs, thereby centralizing most of the connection to the international internet. The government retains a degree of control over the country's internet backbone, and all traffic within the country must flow through a government-controlled telecommunications hub.

ICT Market

The ICT sector is regulated under Law No. 13 of 1995 and its amendment, Law No. 8 of 2002. The law endorses free-market policies and governs licensing and quality assurance.\textsuperscript{17} Citizens and businesses can obtain internet access through privately owned service providers without state approval or registration. A November 2011 reports listed 16 active internet service providers (ISPs) in Jordan, though licenses have been granted to over 20 companies.\textsuperscript{18} The market is dominated by Umnia (a subsidiary of Batelco Bahrain), Zain, and Jordan Telecom, in which France Telecom owns 51 percent of shares, with the remaining shares divided between the Social Security Corporation, the armed forces, and others.

3G services were first launched by Zain and Jordan Telecom (Orange) in mid-2010 and increased upon implementation of a tax exemption for the purchase of smartphones and the launch of mobile broadband by another provider, Umnia.\textsuperscript{19} A call from the TRC to introduce a fourth mobile operator in December 2012, however, was rejected by Zain and Jordan Telecom.\textsuperscript{20} No new providers have been introduced since then and the three companies have a similar share of the market.\textsuperscript{21} After rejecting two international operators, the Jordanian government awarded Zain Jordan with the rights to introduce 4G services to the market. Zain launched its 4G/Long Term Evolution (LTE) services on February 14, 2014. In January 2015, Orange Jordan was awarded the second 4G license for US$100

\textsuperscript{17} “Jordan,” in One Social Network With A Rebellious Message, Arabic Network for Human Rights Information, 2009, \url{http://bit.ly/1V0uqvC}.
\textsuperscript{18} International Telecommunications Union, ICT adoption and prospects in the Arab region, Summit 2012, 57, \url{http://bit.ly/1KuSt2C}.
\textsuperscript{21} Mai Barakat, “Jordan will be challenging, but a fourth operator might find elbow room as a mobile broadband provider,” Ovum, February 21, 2013, \url{http://bit.ly/1BMHl1q}.
Jordan

million and launched LTE services in Amman in May 2015. It announced aims to expand the service nationwide by the third quarter of 2015.22

Regulatory Bodies

The TRC is the independent agency responsible for regulating the ICT sector. It is governed by the Telecommunications Law and defined as a “financially and administratively independent juridical personality.”23 Nonetheless, it is accountable to the Ministry of Information and Communication Technology (MoICT), which was created in April 2002 to drive the country’s ICT development.24 The TRC’s Board of Commissioners and its chairman, currently Ghazi Salem Al-Jobor (appointed in June 2015),25 are appointed by a resolution from the Council of Ministers based on a nomination from the prime minister.26 Although one of the TRC’s responsibilities is to monitor quality of service, its reports rely on self-evaluation reports submitted by the ISPs themselves, in which, for example, Orange Jordan claims that 99.9 percent of complaints are solved within 10 days of receipt. In March 2015, French telecoms company Orange brought a case before the International Centre for Settlement of Investment Disputes against Jordan for a lack of transparency in the procedure for renewing a 2G license.27

Limits on Content

The blocking of news websites has increased since June 2013, when some 300 sites were blocked for failing to obtain a license with the government after a new Press and Publication Law was passed nine months earlier. Since then, most news sites have obtained licenses and had access restored. Over the past year, however, authorities have once again targeted online news outlets with blocking, this time for publishing content surrounding the Jordanian military and its campaign against ISIS.

Blocking and Filtering

On the eve of December 25, 2014, the Attorney General issued a decree prohibiting media outlets from publishing any news or images released by ISIS about Moath al-Kasasbeh, a Jordanian pilot held captive by the terrorist group.28 One day later, the licensed website Al-Kawn News was blocked for disobeying the order and publishing news about the pilot’s captivity circulated by ISIS.29 Al-Kawn News was unblocked four days later, on December 29, 2015, but the news item in question was removed.

On January 28, 2015, Jordanian authorities blocked the licensed local news website Saraya News after it published a report stating that an imprisoned Iraqi militant would be freed in a hostage nego-

Jordan

The website was unavailable for 40 days, during which two staff were detained (see “Prosecutions and Detentions for Online Activities”).

Reacting to these events, Amjad Al-Qadi, the head of the Media Commission, sent a memo on April 6, 2015 to all owners and editors of licensed news websites instructing them not to publish any news or information related to the military without a “clear and direct request to the authorized military sources.” The request was delivered through an email sent to website owners and editors. By contrast, there were no reports that print and audiovisual media received any requests, most likely since they are known to be monitored by the authorities, and their employees do not dare to publish any unauthorized news about the military.

Under amendments to the Press and Publications Law (PPL) passed in 2012, news websites are required to obtain a license from the Media Commission or face blocking. The law also requires any electronic publication that publishes domestic or international news, press releases, or comments to register with the Ministry of Commerce and Industry. One of the requirements for a general news website to obtain a license is to have an editor-in-chief who has been a member of the Jordan Press Association (JPA) for at least four years. The problematic situation eased in July 2014, when the JPA law was amended to enable journalists in online media to become members. Prior to that, journalists could only become members if they underwent a period of “training” in an “official” media organization. According to the Center to Defend Freedom of Journalists (CDFJ), around 500 journalists in Jordan are not members of the JPA.

For many observers, the law's broad definition of a news website includes almost all Jordanian and international websites, blogs, portals, and social networks. According the amended PPL, an electronic publication is defined as “[a]ny website with a specific web address on the internet which provides publishing services, including news, reports, investigations, articles, and comments, and chooses to be listed in a special register maintained at the Department, pursuant to instructions issued by the Minister for this purpose.” Articles 48 and 49 enable the head of the Media Commission to block any website for failing to obtain a license or, more broadly, for violating Jordanian law.

Consequently, 291 news websites were blocked in June 2013 on instructions from the head of the Media Commission (then-named the Press and Publications Department) after a nine-month grace period. Most have since applied for a license to get unblocked. By June 2014, there were 160 licensed general news sites and 100 specialized websites. To obtain licenses, most general news websites hired new chief editors who were already JPA members, a concerning development for independent media given that 64 percent of JPA members work in government or government-related media outlets. Out of 160 licensed websites, 68 hired new editors-in-chief who have full-time jobs at other media outlets, a violation of Article (23-A) of the PPL. As of October 2014, 112 websites were blocked, but only 15 remained operational—the remaining had shut down.

Some unlicensed websites have resorted to using alternative domains in order to remain accessible in Jordan, such as JordaniansVoice.net and 7iber.com. But in June 2014, the newly appointed head

---

31 The report author received a copy of the email.
Jordan

of the Media Commission sent a request to the TRC to block the alternative domains, which in turn sent a decree to ISPs to implement the blocking. In addition, the head of the Media Commission pressed charges against 7iber two months later for operating an unlicensed media organization in violation of Article 48(B) of the PPL. The case is currently in court, and 7iber faces a potential fine of JOD 1,000–5,000 (US$1,500–7,500).

The Jordanian government claimed that the amendments were introduced “to regulate the work of news websites and in order to increase transparency and accountability.” Officials stated that the law was called for by professionals within the industry, in order to preserve professionalism and protect the media from those “who have practiced embezzlement, defamation and blackmailing to a degree that threatened social peace.” On the other hand, local journalists, international human rights groups, and a former Jordanian minister of media affairs and communication criticized the decision as a serious affront to freedom of the press and a decisive move to censor the internet in Jordan.

Content Removal

The 2012 amendments of the PPL increased the liability of intermediaries for content posted on their sites, placing readers’ comments under the same restrictions as normal news content. Clause 3 of Article 49 states that both the editors-in-chief and owners of online publications are legally responsible for all content posted to the site, including user comments. Moreover, websites must keep a record of all comments for six months after initial publication and refrain from publishing any “untruthful” or “irrelevant” comments. As a result, some news websites, such as JO24, stopped allowing comments altogether as an expression of protest.

Media, Diversity, and Content Manipulation

Many journalists and editors practice self-censorship and rarely cross the standard red lines, particularly concerning material that could be perceived as harmful to national security, national unity, the country’s economy, or the royal family. In a 2014 survey of journalists conducted by Center for Defending Freedom of Journalists in Jordan, 91 percent of Jordanian journalists admitted to practicing some form of self-censorship, with more than three-quarters indicating they avoid publishing any material critical of the military, the judicial system, tribal leaders, and religion.

In August 2014, after parliament voted to pass constitutional amendments proposed by the government that give the king sole authority to appoint heads of the military and the intelligence, major

41 In a discussion about the impact of website licensing and the PPL, publisher of news website JO24 Basel Okour said that they stopped allowing comments on their website in protest of the law and to protect the privacy of their readers. See “An Open Meeting at 7iber to Discuss the State of Online Journalism After the Website Registration Requirement,” [in Arabic], YouTube video, 1:43:44, posted by Jordan Days, December 8, 2014, https://www.youtube.com/watch?v=MJUkuFqCBI.
Jordan

newspapers in Jordan did not publish any articles critical of the amendments, demonstrating the high degree of self-censorship in the traditional media. In one incident, prominent journalist and writer Rana Sabbagh wrote on her Facebook profile that her bi-weekly column in Al-Ghad newspaper was banned by the editor, and that she would publish the column on Facebook and in another media outlet.43

The online information landscape was also limited by direct bans on reporting on certain topics. On April 6, 2015, the head of the Media Commission sent a memo to all news websites prohibiting them from publishing anything related to the military without direct approval from the Armed Forces. He wrote in the memo that “websites should refrain from publishing or broadcasting any articles or military information without getting this news or information from official sources in the Armed Forces.”44 Months earlier, on November 26, 2015, the Armed Forces appointed for the first time an official spokesperson, following increased media coverage of Jordan’s participation in the U.S.-led coalition against ISIS.45 However, this did not result in increased transparency from the Armed Forces, as the number of comments and statements made by this spokesperson regarding the war on ISIS was only four, and he did not make any statements regarding Jordan’s participation in the Saudi-led coalition against Yemen.46

Social media applications such as Facebook, Twitter, and YouTube are very popular, particularly among younger Jordanians. Facebook tops the list of most visited websites in Jordan, while YouTube comes in fourth.47 There are around three million Facebook users in Jordan, representing close to half of the country’s population,48 with a penetration rate of 48 percent of the population as of May 2014, of whom 59 percent are male.49 Twitter has garnered a much smaller following of around 161,000 users, or around 2.4 percent of the population.50 State officials, including the Royal Hashemite Court,51 the Queen, the Crown Prince,52 and Prince Hassan,53 have established social media accounts to communicate with the public. Queen Rania is by far the most popular of these accounts, with nearly 4 million followers on Twitter and over 600,000 on Instagram.54 She was, in fact, referred to by Forbes Middle East magazine as “The Queen of Social Media.”55 Among government officials, Foreign Minister Nasser Judeh has over 71,000 Twitter followers, while an unverified account related to Prime Minister Abdulla Ensour has 5,000 followers.56

44 The researcher obtained a copy of the official memo.
49 “Citizen Engagement and Public Services in the Arab World: The Potential of Social Media,” Arab Social Media Report.
50 “Citizen Engagement and Public Services in the Arab World: The Potential of Social Media,” Arab Social Media Report, Figure 32.
56 Prime Minister Dr. Abdulla Ensour Twitter Page, https://twitter.com/DrEnsour.
Digital Activism

In the past year, activists have used social media to advocate for social issues and push for legislative change. On May 2, 2015, activist Reem Al-Jazi wrote an op-ed to protest the fact that hospitals require the approval of the father or a male guardian before admitting a child, even for emergency procedures, and do not acknowledge the mother.57 Her article went viral and sparked a social media campaign petitioning parliament to amend article 123 of the Civil Law that only grants guardianship to the father or the paternal grandfather or uncle.58

Social media platforms, in addition to news websites, have played an important role in mobilizing public protests to oppose restrictions on free expression, to call for broader political reforms, and to protest government policies. Over 500 websites went offline on August 29, 2012 in a coordinated protest against the changes in the PPL.59 The home pages of these sites displayed a black screen with text reading, “You may be deprived of the content of this site under the amendments of the Jordanian Press and Publications Law and the governmental internet censorship.” Nonetheless, social media activism and numerous protests ultimately failed to halt passage of the bill in September 2012.

On the other hand, social media platforms were also utilized to mobilize for further restrictions on access to internet content by users. For instance, a Facebook campaign to press the government to block pornographic websites in the country has garnered more than 37,800 likes as of May 2014.60 The government responded in 2013 by introducing a new telecommunications law that, if passed, would prohibit ISPs from allowing users to access pornographic websites.61 The ICT minister at the time, Dr. Azzam Slait, reportedly withdrew the proposed law, sending it back for further consideration and possible amendments in mid-2014.62 The law was also published on the Legislation and Opinion Bureau’s website to solicit feedback from the public.63

Violations of User Rights

A host of repressive laws and severe punishments create an environment of fear in Jordan, where journalists, political activists, and ordinary users face arrest and possible prosecution if they overstep the boundaries of acceptable speech. Since the passage of the amended antiterrorism law in 2014, a growing number of citizens have faced charges before the military-dominated State Security Court for their online activities, particularly on Facebook.64 At the same time, strict penalties for criminal defamation against public authorities, both foreign and domestic, remain a prominent concern.

---

58 Reem Al Jazi, “Petition my son’s life is my responsibility,” May 2015, http://chn.ge/1SBn85R.
Jordan

Legal Environment

In September 2011, responding to public discontent, constitutional amendments were introduced to strengthen checks and balances and ensure greater protections for human rights. The measures resulted in the creation of a constitutional court (Article 58–61), an explicit prohibition on torture (Article 8), and the restriction of the State Security Court’s jurisdiction to crimes of treason, espionage, and terrorism (Article 110). The Constitutional Court’s nine members were named by King Abdullah II in October 2012. Several constitutional amendments touched directly or indirectly on internet freedom. Specifically, terms such as “mass media” and “other means of communication,” which likely encompass online media, were added to provisions that protect freedom of expression and concomitantly allow for its limitation during states of emergency (Article 15). With regard to the right to privacy, judicial approval was added as a precondition for censorship or confiscation of private communications (Article 18). Despite the passage of an Access to Information Law in 2007, a number of restrictions remain on requesting sensitive social and religious content.

Beyond these constitutional protections, several laws that hinder freedom of expression and access to information remain on the books. These include the 1959 Contempt of Court Law, the 1960 penal code, the 1971 Protection of State Secrets and Classified Documents Law, the 1992 Defense Law, the 1998 Jordan Press Association Law, and the 1999 Press and Publications Law. Defamation remains a criminal offense under the penal code. Amendments to the press law enacted in 2010 abolished prison sentences for libelizing private citizens. However, the same bill increased fines and jail sentences for defaming government officials to up to JOD 10,000 (US$14,000) and 3 to 12 months imprisonment.

The 2010 cybercrime law prescribes penalties for hacking and online identity theft, though it also contains several provisions that could be easily used to suppress online expression. For example, the law prohibits posting any information concerning national security, foreign affairs, the national economy, and public safety that is not already available to the general public. Nevertheless, following protests by civil society, several more egregious provisions related to defamation and warrantless police searches were removed by royal decree in September 2010, one month after the law was passed.

The Press and Publication Law, amended in 2012, bans the publication of “material that is inconsistent with the principles of freedom, national obligation, human rights, and Arab-Islamic values.” Article 38 of the PPL also prohibits any “contempt, slander, or defamation of or abuse of” religions or

69 For example, the law bars public requests for information involving religious, racial, ethnic, or gender discrimination (Article 10), and allows officials to withhold all types of classified information, a very broad category (Article 13) see, Arab Archives Institute, “Summary of the Study on Access to Information Law in Jordan,” June 2005, http://www.alarcheef.com/reports/englishFiles/accessToInformation.pdf.
72 The Press and Publications Law 1998 amended by Law No. 32.
prophets. The same article prohibits the publication of any material that is defamatory or slanderous of individuals who are also protected by the same law against "rumors" and "anything that hinders their personal freedom."\textsuperscript{73} Journalists, website owners, and editors in chief face a fine of JOD 5,000 (US$7,500) if found to violate the law. In addition, civil defamation suits against private individuals can result in fines of between JOD 500 to 1,000 (US$700 to 1,400).\textsuperscript{74}

In early 2014, a law was passed to limit the powers of the quasi-military State Security Court, before which citizens and journalists could be tried for crimes related to freedom of expression. The law, proposed in September 2013 in response to international criticism, limited the court’s jurisdiction to only five areas: terrorism, espionage, drug felonies, treason, and currency counterfeiting.\textsuperscript{75} At the time, the changes were seen cosmetic at best, with Human Rights Watch stating that Jordan needed to “overhaul its outdated penal code and stop dragging civilians in front of the State Security Court just for demonstrating for reform.”\textsuperscript{76}

Worryingly, amendments to the 2006 antiterrorism law passed in mid-2014 essentially reversed many of the advances made in the above-mentioned law by expanding the definition of “terrorism” to include broader offenses.\textsuperscript{77} Sanctioned by the senate on May 1, 2014\textsuperscript{78} and endorsed by King Abdullah II the following month,\textsuperscript{79} the amendments have been criticized for “broaden[ing] the definition of terrorism and threaten[ing] freedom of expression,”\textsuperscript{80} while increasing the scale of punishments. In addition to more legitimate offenses such as attacking members of the royal court or provoking an “armed rebellion,” the definition of terrorist activities now includes any acts that “threaten the country’s relations to foreign states or expose the country or its citizens to retaliatory acts on them or their money,” an offense that had already been listed in the penal code.\textsuperscript{81} The new law also explicitly penalizes the use of information and communication technologies (ICTs) to promote, support, or fund terrorist acts, or to subject “Jordanians or their property to danger of hostile acts or acts of revenge.”\textsuperscript{82}

Political analysts understood the new amendments in the context of the security threats posed by Jordan’s proximity to Syria and growing tensions in the region.\textsuperscript{83} However, many critics view the bill as a tool for the government to crackdown on the opposition and impose further restrictions on media freedom.\textsuperscript{84} Online media outlets will be even more hesitant to publish any news or opinions that could be construed as overly-critical of foreign leaders or diplomats, particularly of foreign countries. The law comes at a time when neighboring countries, such as Egypt,\textsuperscript{85} Saudi Arabia,\textsuperscript{86} and the Unit-

\textsuperscript{73} Law number (32) 2012. Amendments to The Press and Publications law for the Year 1998 (8), Article 38, clauses A, B, C & D.
\textsuperscript{74} The Press and Publications Law 1998 amended by Law No. 32.
\textsuperscript{76} Human Rights Watch, "Jordan: End Trials of Persecutors Undermining Regime.”
\textsuperscript{80} Human Rights Watch, "Jordan: Terrorism Amendments Threaten Rights.”
\textsuperscript{81} Anti-Terrorism law –No 18 2014 Article 3 (b), http://bit.ly/1rDOKp.
\textsuperscript{85} Shadia Nasralla, “Egypt designates Muslim Brotherhood as terrorist group,” Reuters, December 25, 2013, http://reut.rs/1cBG3C.
ed Arab Emirates, have outlawed the Muslim Brotherhood as a terrorist organization. The Islamic Action Front, the political arm of Jordan’s Muslim Brotherhood and a prominent opposition group, asked for changes to the law to be made in early 2014.

Prosecutions and Detentions for Online Activities

Several journalists have been charged with criminal offenses despite provisions in the Press and Publication Law that ban the jailing of journalists for press offenses. On January 28, 2015, Jordanian authorities arrested Saraya News owner Hashem Al-Khalidi and editor Saif Obeidat after the news site published a report stating that an imprisoned Iraqi militant would be freed in a hostage negotiation deal with ISIS. The two were charged by the State Security Court of using media to spread the ideas of a terrorist group and of placing Jordanians under threat of hostile acts in violation of articles (3) and (7) of the amended antiterrorism law. They were detained for 40 days before being released on bail, after which point the website was unblocked.

Political tensions have also resulted in the prosecution of Jordanians affiliated with the Muslim Brotherhood. In November 2014, the deputy leader of the Muslim Brotherhood in Jordan, Zaki Bani Irshaid, was arrested and charged with “harms Jordan’s ties with a friendly state” under the amended antiterrorism law after he published a post on his Facebook profile criticizing the UAE government and accusing it of sponsoring terrorism and supporting the “Zionist agenda.” He was repeatedly denied bail during the trial, and in February 2015 he was sentenced by the State Security Court to 1.5 years in prison with hard labor. The Court of Cessation upheld the ruling in April 2015.

In January 2015, two activists affiliated with the Muslim Brotherhood were arrested on orders from the State Security Court because of material they published on Facebook. Thabet Assaf was arrested on January 15 and charged with “undermining the regime on social networking websites.” He was released on bail on March 26. Basem Rawabdeh was arrested on January 17 and charged with “inciting to oppose the regime through Facebook comments.” He was sentenced to five months in prison and released in May 2015.

Even parliamentarians (MPs) have been targeted for their online posts. In March 2015, two citizens filed a complaint against MP Tarek Khoury at the State Security Court for a Facebook post in which he criticized Jordan’s peace treaty and relationship with Israel. Following the complaint, the State Security Court prosecutor sent a request to the prime minister requesting that parliamentary immunity be lifted from Khoury in order to put him on trial for charges of “undermining the regime”

95 The researcher obtained a copy of the military prosecutor’s letter to the Prime Minister.
and “using the internet for acts no sanctioned by the state that can harm the Kingdom’s ties with a foreign country” under articles (3-B) and (7-C) of the antiterrorism law. The two citizens who filed the complaint eventually withdrew it, but many viewed the move as a message intended to deter people from expressing their views freely on Facebook.

**Surveillance, Privacy, and Anonymity**

Since the passage of amendments to the antiterrorism law in 2014, a number of people have been arrested and put on trial at the State Security Court for private messages they posted on WhatsApp. While there is no concrete evidence that the government systematically monitors and intercepts private communications, defense lawyers say that material obtained from mobile phones or laptops is often obtained without a court order, which cannot be legally used as evidence. In October 2013, Ayman al-Bahrawi was accused of “lengthening the tongue” and “insulting” foreign heads of state in private WhatsApp messages found on his mobile phone.

In general, Jordanians are careful when talking on mobile phones or at public meetings. This attitude has passed naturally to the internet, where it is believed that security services closely monitor online comments, cataloging them by date, internet-protocol (IP) address, and location. Furthermore, clauses within mobile phone contracts give Jordanian companies the right to terminate services should customers use it in any way “threatening to public moral or national security.”

Cybercafes, where users might otherwise write with relative anonymity, have been subjected to a growing set of regulations in recent years. Since mid-2010, operators have been obliged to install security cameras to monitor customers, who must supply personal identification information before they use the internet. Cafe owners are required to retain the browsing history of users for at least six months. Authorities claim these restrictions are necessary for security reasons. Although enforcement is somewhat lax, the once-thriving cybercafe business is now in decline due in part to the restrictions, as well as increased access to personal internet connections.

**Intimidation and Violence**

There were no reported instances of physical violence against internet users for their online activities over the past year. A climate of fear and intimidation remains, however, for those working in online media. The last reported incident occurred on July 17, 2012, when unknown perpetrators raided the offices of the online news site Watan, stealing documents and damaging equipment.

**Technical Attacks**

Over the past year, incidents of cyberattacks against bloggers and staff of online news websites de-

---

Jordan

creased in severity compared to previous years. In 2012, the webpages of the news sites Khbereni and Al Ain were hacked; the site of the Jordanian rap group Ahat was also hacked on September 15, 2012. In February 2011, one of the country’s most popular news websites, Ammon News, was hacked and temporarily disabled after its editors refused to comply with security agents’ demands to remove a statement by 36 prominent Jordanian tribesmen, in which they called for democratic and economic reforms. Among other actions, the hackers deleted the joint statement, which were politically sensitive given the groups’ historic support for the monarchy.

Key Developments: June 2014 – May 2015

- Following ethnic clashes in the South Kazakhstan region in February 2015, the government temporarily disconnected internet service and blocked mobile phone networks in the area (see Restrictions on Connectivity).

- The government blocked pages and entire websites of foreign and domestic news outlets for reporting on Kazakh nationals fighting for ISIS, which it characterized as propaganda (see Blocking and Filtering).

- Amendments to the criminal code, which were passed in May 2014 and went into effect in January 2015, criminalized the dissemination of rumors and increased punishments for libel, including harsher penalties for online content (see Legal Environment).

- A court decision in September 2014 banned any websites or tools that allow users to hide their internet protocol (IP) addresses (see Surveillance, Privacy, and Anonymity).
Kazakhstan

Introduction

The state of internet freedom in Kazakhstan continues to decline, as the government increasingly cracks down on independent journalism and online content deemed “extremist,” ranging from content critical of the government to news reports about Kazakh involvement with ISIS. The government also continues to pass restrictive laws banning certain content online and expanding its powers to shut down communication networks and media outlets.

In 2015, amendments to the criminal code came into force that toughened penalties for defamation and introduced criminal liability for the dissemination of rumors. Earlier, in May 2014, the government granted the office of the prosecutor general the right to shut down websites, block access to pages, or disable telecommunications services entirely if they are used for malicious purposes. These laws were employed repeatedly during the coverage period to target both local and international online media, as well as to disconnect areas in South Kazakhstan from the internet and mobile networks in the aftermath of ethnic clashes.

For over a decade, the Kazakhstani government has shown a keen interest in the development of the information and communication technology (ICT) sector, seeing it as a way to diversify the country’s extractive economy. It has not brought about any noticeable innovation, but showed relative progress in increasing access to internet and mobile telephony, and setting up national data centers and e-government resources.

The government has employed a set of technical and legislative measures to control content both directly and through the establishment of a pervasive atmosphere of self-censorship online. This approach has been consistently implemented in the past few years, replacing the earlier paradigm of building a strong ICT cluster that would be able to develop national analogs of foreign social networks, blogging platforms and even search engines.

Obstacles to Access

The government of Kazakhstan consistently works on improving ICT infrastructure together with the national operator, Kazakhtelecom, which further solidified its dominant standing in the market during the reporting period. Technological upgrades were accompanied by tightening centralized control of both state-owned and private telecommunication networks, including legal changes that enabled the authorities to shut down entire communication networks, platforms, or applications. Several instances of short-term disruptions in access occurred in the reporting period.

Availability and Ease of Access

With the investment that the government and Kazakhtelecom is making to improve both the backbone and “last mile” infrastructure, obstacles to a free-flowing internet have less to do with infrastructural capacity and more to do with government decisions to limit access. Internet access has grown significantly in Kazakhstan over the past few years, increasing from a penetration rate of 18 percent in 2009 to 55 percent in 2014, according to the International Telecommunication Union (ITU).¹ Official government statistics consistently inflate this indicator, and experts question these

Kazakhstan

figures, citing a lack of clarity in the methodology. In July 2014, the head of the Agency for Communication and Information claimed that internet penetration had exceeded 70 percent. In September, he announced that the internet is being used already by 12 million Kazakhstans aged 16-74 (75 percent of the population). Experts believe that the government arrives at these numbers by counting not the number of people, but the number of devices connected to the internet or points of access and multiplies them by the average number of potential users. Data from the Ministry of Investments and Development indicates that the number of households with an internet connection in 2014 was around 2 million (with 99 percent of them having broadband access; the Committee for Statistics puts this figure at 43 percent, indicating that 32.5 percent of users connect via ISDN), and the number of business enterprises with internet connection was below 60,000.

Official statistics do not provide the data breakdown for urban versus rural connections, but access is more limited for rural areas, where 45 percent of the population resides. The regional split shows that Almaty—the most populous city and the business and cultural center of Kazakhstan—accounts for more than 35 percent of internet users, and for more than 55 percent of the ICT industry’s revenue.

Most people access the internet from home, alongside increasing free access at educational institutions, workplaces, and public places, including pilot projects offering Wi-Fi access on public transport vehicles in several cities in 2014. Internet speeds offered by Kazakhtelecom and private ISPs did not change significantly over the past year, but the national operator doubled the speed of access to domestically-hosted websites (up to 4 Mbps) for one of its popular budget tariff plans in July 2015 and planned to lower the wholesale prices for secondary ISPs. Its main rival in the retail sector, Beeline, continued investing in the development of independent fixed-line infrastructure, and did not introduce any changes (it offers 25-100 Mbps packages for fees similar to those of Kazakhtelecom). The average connection speed, estimated by the Akamai “State of the Internet” Report, was 5.1 Mbps in the fourth quarter of 2014.

The mobile phone penetration rate reached 168 percent in 2014, according to the ITU. According to J’Son & Partners consultancy, mobile internet penetration in Kazakhstan was at 67 percent in 2013. Official data specifies that in 2013, nearly 30 percent of all internet connections were

---

Kazakhstan

made with GPRS, WAP, or other wireless technologies, and 21 percent with mobile broadband connections.16

Kazakhstan’s multi-ethnic demographics and the prevalence of the Russian language from the Soviet era do not have significant impact on access: all public institutions are required to provide two language versions on their website, and many private sector actors follow this trend, although currently there is much more domestic content available in Russian than in the Kazakh language. A more significant obstacle to the further proliferation of access is its affordability. Both state and private ISPs prefer to upgrade the speed of connectivity while keeping the tariffs fixed, rather than lowering prices. Kazakhtelecom’s unlimited broadband (4 Mbps) subscriptions currently start from US$20 to $25 per month; Beeline’s cheapest unlimited contract (25 Mbps) costs $18 per month. In both cases the advertised speed refers to domestic traffic. Unchanged tariffs appear to be slightly lower than in the previous year because of the 20 percent currency devaluation in 2014, but they still are high when compared to the average monthly income, which was approximately US$643 as of November 2014,17 10 percent lower than the U.S. dollar equivalent in November 2013. Access to domestic and external resources does not vary in price, only by speed of access provided.

Restrictions on Connectivity

The government imposes no restrictions on the bandwidth of access offered by ISPs, but it centralizes the infrastructure in a way that facilitates control of content and surveillance. Over the past year the government placed restrictions on ICT access in South Kazakhstan during riots in February 2015. Internet users also reported disruptions in several communication applications throughout the year, though the cause of these disruptions remains unverified.

In February 2015, the government temporarily shut down mobile phone and internet services for the first time since regulation authorizing such actions was passed in 2014. Internet and mobile telephony services were shut down in several areas of the South Kazakhstan oblast, including in Shymkent, Kazakhstan’s third largest city, in order to “prevent rumors,” shortly after ethnic violence erupted in two villages in the region.18 The block was gradually lifted and limited to the conflict-hit zone, where it lasted for nearly a week.

In 2012, amendments to the Law on National Security allowed the government to forcibly suspend telecommunications during anti-terrorist operations or the suppression of mass riots.19 Further legislation was passed to compel private actors in the field—websites, ISPs or mobile operators—to follow the government’s orders when it comes to blocking or disconnecting service. In April 2014, the government formalized its right to shut down ICTs or access to pages at the discretion of the prosecutor general’s office without a court order if “networks are used for felonious aims to damage the interests of individuals, society or state,” including the dissemination of illegal information, calls for extremism, terrorism, mass riots, or participation in unauthorized public gatherings.20 This regulation

implies that limitations may be applied to the use of telephony, text messages, and instant messaging applications. The law makes either telecom operators or the State Technical Service responsible for the implementation of the prosecutor’s order. Prior to the regulation, it was assumed that the government had taken such actions in the past, though this had not been confirmed. In 2011 the government reportedly acquired technology allowing for localized disruption of communications and blocking of unwanted online content, and used it during the Zhanaozen riots. It is not clear which body operates this technology, the National Security Committee or the State Technical Service.

Kazakhtelecom, through its operations and through a number of subsidiaries, holds a de facto monopoly on external backbone channels; Beeline is the only independent backbone provider. The Traffic Exchange Point—a peering center, established by Kazakhtelecom in 2008—is meant to facilitate service among first-tier providers, but in 2010, it turned down Beeline’s application to join the pool without giving any reason. Beeline submitted a repeated request in February 2015, but it was rejected, citing deficit of capacity.

ICT Market

The state (through the sovereign wealth fund “Samruk-Kazyna”) owns 52 percent of Kazakhtelecom, the largest ISP in Kazakhstan, with a 70 percent share in the broadband internet market. It fully or partly owns a number of other backbone and downstream ISPs, and the overall market share is difficult to estimate. Beeline, by its own estimates, accounts for 13.1 percent of the broadband internet market.

Kazakhtelecom uses its dominance to distort the market. For example, the government continues to support Altel’s monopoly over the 4G LTE network (Altel is owned by Kazakhtelecom) and plans to continue doing so until 2018, citing the alleged lack of frequencies and the need to accomplish the digital switchover process. This has allowed Altel, previously a dormant CDMA operator, to quadruple its user base, though it still holds a relatively small share of the mobile market. In December 2014, the state-owned Kazakhstan Bank of Development provided a 10-year credit of over US $560 million to Altel for the expansion of its 4G network. The money came from the National Fund, a savings and stabilization fund that generates oil revenues. In April 2015, the government said it is considering allowing mobile operators to provide 4G services in a “technologically neutral mode,” using the frequency spectrum they already have, starting in 2016.

As of March 2015, there were four mobile telephone service providers in Kazakhstan, three of which use the GSM 3G standard (Kcell, Beeline, and TELE2). All GSM operators are privately owned, with large foreign participation in ownership. Kazakhtelecom has fully owned Altel since 2006.

22 Email interview with a Beeline representative. March 2015.
24 Email interview with a Beeline representative. March 2015.
Regulatory Bodies

There is no independent body holding a regulatory mandate to oversee the internet in Kazakhstan. The Internet Association of Kazakhstan (IAK), established in 2009 in the form of a union of legal entities, claims to unite the Kazakh internet community to participate institutionally in the political decision-making process, yet experts question the group’s independence, transparency, and non-profit status.29 The association does not have an official government mandate but actively cooperates with the prosecutor general’s office on “fighting illegal content”30 and on a variety of other issues, including content filtering and the collection of personal data of users leaving comments on news sites, according to emails released by hackers from an account belonging to IAK president Shavkat Sabirov.31 The leaks were posted online in January 2015 by Muratbek Ketebayev, a former journalist within the opposition media, residing in Europe, who claims that the leaks were a matter of public interest. In an interview to Ratel.kz, Sabirov confirmed the authenticity of emails, but declined to elaborate on the allegations of his close cooperation with the law enforcement bodies, including possible assistance in revealing the identities of commentators on news sites.32

The agencies officially authorized to supervise the ICT sector are reorganized periodically together with the rest of the government in frequent attempts to optimize their operations. The most recent changes were introduced in 2014; in March, the president issued a decree forming the Agency for Communication and Information to manage issues of communication, information, and archives. But as early as August, another decree reshuffled the whole government, and the regulation of the media, internet and technology sector was given to the newly formed Ministry of Investments and Development. Its Committee for Communication, Informatization and Information is an official body designated to hold “regulatory, operational and controlling functions” in the entrusted areas.

The “.kz” top-level domain is managed by a registry, the Kazakhstani Network Information Center (KazNIC), and the Kazakhstani Association of IT Companies. KazNIC, based in provincial town of Semey in Eastern Kazakhstan, was created in 1999. The Kazakhstani Association of IT Companies was created in 2004, also as a noncommercial entity to administer the infrastructure of the national domain zone. In January 2015, it issued an order doubling the minimum price of a .kz domain.33 Both organizations are believed to be under indirect control of the authorities.34 Since 2005, the government has required that any website with a “.kz” country domain be hosted on servers within the territory of Kazakhstan.

Limits on Content

The authorities have established numerous legal means to restrict online content. The most frequent reason they use to justify restrictions to online content is extremism; however, the courts review those applications in bulk and the proceedings are not transparent. Moreover, this year it has become a common practice among the state bodies to request the pre-trial blocking of online content listed in

---

32 Ibid.
Kazakhstan

a lawsuit, which the courts readily satisfy. The most significant cases of censorship in 2014-2015 were related to domestic and international coverage of Kazakhstan’s connection to ISIS. The law passed in April 2014 granting the prosecutor general’s office the right to issue blocking orders without a court decision has been used extensively to block or force the deletion of content. The authorities continue to pour funds into supporting online media outlets disseminating progovernment content, and allegedly to help institute the Bloggers Alliance of Kazakhstan, which is generally viewed as a progovernment enterprise.

Blocking and Filtering

The government possesses extensive legal means with which to justify blocking online content. According to the country’s media law, all internet resources, including websites and pages on social networks, are considered media outlets. Decisions to suspend or close media outlets are supposed to be made by courts, but in 2014, amendments were introduced granting the prosecutor general’s office the authority to order the blocking of websites without a court decision if the websites are found to be hosting illegal content. ISPs must conform to such requests until the website owner deletes the content in question. The law provides no space for an ISP to reject the order or for the website owner to appeal.

Unverified outages of certain online platforms were reported during the coverage period. On August 23, 2014, users reported disruptions in access to social media platforms, including Twitter, Facebook, Instagram, and VKontakte, for nearly three hours during the night. Local forum Vse.kz was loading, though at a slower speed. On November 25, users complained of intermittent access to Gmail, and reported that Google’s banner ads network was not displayed on websites. Users in the eastern part of Russia reportedly experienced the same problems. On November 27, multiple users again reported outages of VKontakte, Facebook, Twitter, Instagram, Youtube, and messenger services WhatsApp and Viber. As in August, the services could not be accessed through any ISPs or mobile operators for several hours, though internet users could connect to the sites through VPNs, indicating that the disruption was not a problem with the platforms themselves. ISPs and officials denied their involvement in blocking. Some observers feared that it could be a testing of the blocking capacity by the government. LiveJournal, a popular Russian-language blogging platform, is still blocked in Kazakhstan since 2008, with a short break between November 2010 and August 2011 in which it was available.

In early May 2015, access to SoundCloud, an international platform for sharing music and podcasts, was blocked in Kazakhstan. ISPs claimed that they were not responsible for blocking SoundCloud, and that it might have been a downstream blocking, possibly due to copyright violations. In late May, journalists obtained an official letter from the Committee for Communication, Informatization and Information under the Ministry of Investments and Development, which said that access was blocked on May 12, 2015, because one of the accounts on SoundCloud allegedly contained extremist materials by the Hizb-ut-Tahrir Islamist group. Officials maintain that it was a “preventive block-

Kazakhstan

ing,” which would be in place until the website’s administration deleted the disputed content, as stipulated in the Committee’s letter. A SoundCloud representative posted on the F.A.Q. page that they are “aware of an ongoing issue in [...] Kazakhstan” and were “attempting to resolve this.”

The courts continue issuing frequent decisions to block websites, banning dozens at a time, mostly on the grounds of religious extremism. Three justices of the Saryarka District Court of Astana are designated to deal with cases related to blocking online content. Judges and prosecutors repeatedly display a lack of technical expertise, banning URLs of irrelevant websites like search engines. Websites can be blocked even in the absence of the defendant's representative; no further notification—to the public or the website owner—about why the website is blocked is required.

At the same time, websites often appear to be blocked without any court decision or prosecutorial request at all. Two major Central Asian news sites, Ca-news based in Kyrgyzstan, and Fergananews based in Russia, are not accessible from Kazakhstan for unknown reasons.

In the fall of 2014, a series of propaganda videos by ISIS portrayed alleged Kazakh nationals, including children, as ISIS soldiers. Kazakhstan was very quick to block all pages where the video itself or reports on it appeared, targeting single pages on the sites Lenta.ru, Vlast.kz, Clashdaily.com and sometimes entire websites including Kloop.kg, and the website of the U.K.-based newspaper, the Daily Mail. After the blocks went into effect, the prosecutor general’s office issued a press release warning against the dissemination of the videos, citing an official decision that made this content illegal. According to media professionals, websites were being blocked “in bulk” for publishing news on Kazakhstani citizens participation in ISIS recruitment. In January, another ISIS video appearing to feature Kazakh nationals was disseminated on the internet, causing another wave of website blocking, including pages with relevant news reports on the major Russian daily site Kommersant.ru and on Azattyq.org (RFE/RL’s Kazakh Service).

Several reports by Azattyq.org and Eurasianet.org about the government’s crackdown on Adam Bol—an independent magazine that reported on human rights and government corruption before it was shut down—and reports about its editor-in-chief’s hunger strike were blocked in November 2014 and January 2015. There were also reports that a YouTube video of the inter-ethnic clashes in the South Kazakhstan oblast in February 2015 was blocked for internet users in Kazakhstan.

Additionally, Ratel.kz, a critical news site that sporadically experiences problems with access, reported in December 2014 that it had been blocked by Kazakhtelecom. Meduza.io, an independent Russian news site, was fully blocked in October 2014 after publishing a story about the possibility of

47 Dina Baidildayeva, activist and Azattyq radio employee, Facebook post, [in Russian], January 30, 2015, http://on.fb.me/1Bm5xhr
48 Dih123, Twitter post, February 6, 2015, https://twitter.com/dih123/status/563694236873535488
Kazakhstan

an eastern Ukraine-style secession of a part of Kazakhstan. The blocking was introduced following a lawsuit from the Committee for Communication, Information and Informatization under the Ministry of Investments and Development. It asked the court to acknowledge the article as extremist content and requested that the website be blocked immediately, before the case was considered by the court.\(^{50}\) It remained blocked at the end of May 2015. Avaaz.org, an international online petitions platform, also remains blocked after an incident in December 2013 when a petition calling for the president’s resignation appeared and quickly became popular; the Ministry of Communications denied making the blocking request in this case.

In August 2014, the Committee for Religious Affairs under the Ministry of Culture and Sport announced that 55 websites had been blocked by court decisions since the beginning of 2014 for content related to propaganda of religious extremism and terrorism. The Committee is reportedly monitoring more than 5,000 websites for such content.\(^{51}\) In January 2015, Prosecutor General Askhat Daulbayev stated that his office monitors over 100,000 web resources, and seeks to block extremist websites hosted in other countries. He cited one instance of such cooperation with his Russian counterparts (related to the January blocking of an ISIS video, mentioned above). In total, the prosecutor general’s office asked courts to ban 703 websites and 198 web articles in 2014, and demanded the pre-trial blocking of many of the websites in question.\(^{52}\) According to a statement by the Committee for Communication, Informatization and Information released in August 2014, their activities since March 2014 included 23 lawsuits requesting blocks on 649 websites and 92 URLs.\(^{53}\)

In March 2015, several weeks before the early presidential elections in Kazakhstan, the Central Election Committee’s vice-chairman Vladimir Foos said that access to social networking websites could be blocked on the eve of the voting day, “if a user would post some campaign materials during the election silence period.”\(^ {54}\) No measures were taken to suspend access to any sites during the campaign or after election day. In October 2014, the government adopted guidelines for the use of the internet by civil servants, public officials, and employees of state-owned companies. In order to “prevent possible threats to the image of civil service, dissemination of false information or leaks as a result of online activities,” the document urges employees to abide by the law, but also demands that individuals not post or repost materials that are critical of the state or state bodies, and not to “friend” people that criticize the government and its policies.\(^ {55}\)

The authorities have also sought to undermine the availability of circumvention tools, but more people have started using methods to circumvent blocking such as VPNs. Facebook, Twitter, YouTube and other international platforms hosting user-generated content are freely available.

### Content Removal

In order to avoid having a website or webpage blocked, individuals must remove content that is deemed extremist or is otherwise banned. On April 23, 2014, a new law “On amendments and ad-


denda to laws governing activity of the internal affairs bodies” granted the prosecutor general’s office the authority to suspend access to websites or particular content on websites without a court decision. Requests for a temporary ban require the Committee for Communication, Informatization and Information to inform ISPs within one hour, after which the blocking must be implemented within three hours. When the publisher of disputed content complies with the removal request, however, the website can be unblocked.\(^{56}\) The takedown process is not transparent, and in some cases the public may only learn about the content removal if users notice and report it on social media or if the online publication makes the case public.

By equating all internet resources with media outlets, the country’s media law makes web publishers—including bloggers and users on social media websites—equally liable for the content they post online, but it does not further specify if online platforms are responsible for the content that is posted there by third parties.

There were several cases of content removal from YouTube, including the video of inter-ethnic strife in the South Kazakhstan oblast in February 2015, and a series of videos filmed by drivers to document the abuse of power by police officers, cases of aggressive behavior, or traffic violations by people with powerful connections. In some of these cases, the content was flagged for removal because of alleged violation of copyright.\(^{57}\)

### Media, Diversity, and Content Manipulation

In addition to blocking and removing content, the online media landscape in Kazakhstan is also subject to less overt forms of restrictions on the free flow of information, such as progovernment propaganda and pressure to self-censor. Self-censorship in both traditional and online media outlets is pervasive. Social media remains the freest environment for the public exchange of news and opinions, but discourse there is considered to be very prone to manipulation and propaganda, including by commentators paid by the government. Although the authorities impose no restrictions on the placement of advertisements on critical websites, the atmosphere of self-censorship extends to businesses too. Moreover, frequent problems with access to such sites due to blocking or, in some cases, DDoS attacks, make it unsustainable to advertise there.

Government procurement contracts in the information sphere reached a record sum of US$250 million in 2014.\(^{58}\) This amount only includes contracts issued by the central government, not counting funds that are distributed by local administrations. Many progovernment online media outlets, including local privately owned blogging platforms, are frequent recipients of such contracts.

The Kazakhstani blogosphere has experienced a decline in popularity over the past few years, with more internet users migrating to Facebook and Twitter. The word “blogger” is commonly used to refer to those on Facebook as well. In 2013, government officials voiced their interest in officially recruiting popular domestic and foreign web publishers, bloggers, and moderators of online communities and supporting—both organizationally and financially—their reporting on state matters.\(^{59}\) The Internet Association of Kazakhstan was reported to be acting as an intermediary in building this

---

\(^{56}\) “ЗАКОН РЕСПУБЛИКИ КАЗАХСТАН,” [Law of the Republic of Kazakhstan].


Kazakhstan

cooperation. In October 2014, a group of relatively popular Facebook users registered the Bloggers Alliance of Kazakhstan to "make the country's information space healthier." It was widely believed to be a regime-inspired initiative, especially since its office is located within the government's headquarters. These suspicions were reinforced by a statement it released in February 2015 calling to replace the early presidential elections orchestrated by the authorities with a referendum to extend the incumbent president's powers until 2022, because, according to the statement, "everyone knows that N. Nazarbayev's historical role makes him uncontested." Many representatives of the online community believed the Alliance was created to mislead the public by appropriating the right to speak on behalf of all Kazakhstani bloggers.

LGBTI people in Kazakhstan are routinely stigmatized and discriminated against, and the situation worsened with a proposed law that would have banned "propaganda of homosexuality to protect children" and was initially passed in parliament. In addition to the influence of similar legislation in Russia, a highly resonant case preceded this move, when a poster depicting two male historical figures kissing each other triggered a media uproar in October 2014. The image, a concept ad for a gay club in Almaty, was submitted by Havas Kazakhstan advertising agency to the Central Asian festival of advertisement in Kyrgyzstan. Its creators maintained that it was not designed for use in actual publicity campaigns, but the image was posted on social media by the festival organizers. A wave of public anger resulted in a suit against the agency from a group of 34 people, whose legal status did not provide them with the right to be complainants in such case. Despite these irregularities, the court fined the agency more than US$180,000 in reparations for insult. Human Rights Watch has condemned the verdict. In May 2015, the Constitutional Council rejected the draft law on "propaganda of homosexuality," citing the "lack of clarity and discrepancies in terminology in Russian and Kazakh versions of the draft law, which left room for the possibility of violation of some constitutional norms." Kazakhstan was aspiring to host the 2022 Winter Olympics, and some saw this move as a compromise in an attempt to win the bid, which had become conditional upon the host country's attitude towards minorities.

Digital Activism

The use of social media platforms and other digital tools to organize for social and political campaigns is limited. In February 2014, after a largely unexpected 20 percent devaluation of the national currency, frustrated citizens shared their reactions online, and two small rallies held in Almaty were coordinated via Facebook and WhatsApp, although the protests soon died out.

A grassroots movement to protest against cuts in maternity benefits and an increase in the retirement age emerged in early 2013. These movements actively employed social media to reach out to potential supporters and coordinate offline activities. In June 2013, Serik Abdenov, the minister of labor and social protection supervising the measures, was fired amid growing public discontent.

---

60 See Kazbek Beisebayev, Facebook post, December 26, 2013, accessed January 14, 2014, [http://on.fb.me/KgC6Mt](http://on.fb.me/KgC6Mt).
Kazakhstan

Yet the need to increase the retirement age has been reiterated by the government, although the process was extended and the maternity benefits issue was not resolved. The movement soon dissipated.

Users continue to actively share postings and comment on various matters, including corruption, controversies in the judicial system, blatant cases of injustice, and others. Still, such conversations rarely transform into offline mobilization. One of the most notable cases of self-organized action that migrated from the online sphere was in response to the April 2015 floods in Central Kazakhstan, when internet users in Almaty and some other cities volunteered to donate and administer humanitarian aid to the victims of natural disaster.66

Violations of User Rights

New amendments to the criminal code, passed in May 2014, include provisions to criminalize the dissemination of rumors—offline and online—with penalties of up to 10 years of imprisonment. The amendments also increased penalties for “knowingly disseminating false information” that may inflict damage, or during “public events.” Despite past pledges to decriminalize libel, the new code increased punishments for defamation. In two controversial cases, individuals were charged with extremism for their posts on Facebook; both were publishing comments on the Russia-Ukraine conflict in the context of its impact on Kazakhstan. Additionally, there is evidence to suggest that the authorities may have intermittently blocked the Tor Project’s anonymization network in Kazakhstan. After a long break in enforcing registration requirements for mobile users, the government began forcing mobile operators to discontinue service to unregistered SIM cards. Additionally, CERT, the Kazakhstani governmental agency for addressing online emergencies, was found to be involved in monitoring and censoring political content.

Legal Environment

The constitution of Kazakhstan guarantees freedom of expression, but this right is conditioned by many other legislative acts and in practice is severely restricted. The criminal code provides stricter punishment for libel or insult of the president and other state officials, judges, or members of parliament. The authorities also use various legislative, economic, and administrative tactics to control the media and limit free speech. Kazakhstani officials have a track record of using defamation charges to punish critical reporting. Additionally, the judiciary in Kazakhstan is not independent from the executive, and the president appoints all judges. The constitutional court was abolished in 1995 and replaced with the constitutional council, to which citizens and public associations are not eligible to submit complaints.

In May 2014, amendments to the criminal code criminalized the dissemination of rumors, or “patently false information, fraught with the risk of breach of public order or imposition of serious damage,” punishable by a fine of up to US$10,000 or up to one year imprisonment. The penalties for the same act, if conducted with the use of mass media or ICT networks (including internet and messaging services), would increase to a fine to US$50,000 and possible imprisonment up to five years.

Kazakhstan

years. If this information inflicted damage to a citizen, legal entity, or state, the punishment increases to US$70,000 and up to seven years in jail. If the rumors were disseminated during emergency, war or public events, the prison term can be extended up to 10 years. A new version of the criminal code was signed into force in July 2014, and kept this article in its entirety. The new code also made punishment for libel harsher, doubled the fine for “libel in public or in the media” to US$20,000, and introduced possible imprisonment for the same offense for up to two years (the previous code provided only for “restriction of freedom” for up to two years).

In May 2013, President Nazarbayev signed the law “On personal information and its protection,” which was criticized by media activists as restrictive for journalism. According to observers, since the law does not distinguish between information relating to private or public individuals, investigative reporters now risk prosecution for violation of privacy charges if they publish information about official corruption.

Although the Kazakhstan media law considers websites as media outlets, in most cases this status applies only when assessing liabilities, without granting these outlets the same rights as traditional media. Officials often refuse to provide information that online news sites are requesting. The rules for journalists’ accreditation at state bodies and public associations, adopted in June 2013, make it impossible for online media outlets without official registration to obtain such accreditation.

Prosecutions and Detentions for Online Activities

The government of Kazakhstan continues to arrest and prosecute individuals for posting political or social commentary online that is deemed critical of or threatening to the ruling regime. Additionally, during the coverage period there were two cases in which internet users were sued for incitement of inter-ethnic hatred:

- In January 2015, Tatyana Shevtsova-Valova was sued by the authorities for her alleged posts on Facebook, which propagated the idea of the “Russian World,” (a loosely formulated ideology of the Russian regime, justifying its claims to greater control over the former Soviet states), insulted Kazakhs, and called for a Crimea-style Russian occupation of Kazakhstan. She faced up to 7 years in jail. In March 2015, the court found her guilty and passed a suspended four-year sentence.

- In March 2015, Saken Baikenov, an activist with the low-key nationalist Antigeptil movement, faced the same charges for his postings on Facebook, commenting on Russia’s policy in the region in a manner considered provocative and including insults toward Russians in general. Unlike Shevtsova-Valova, who was allowed to remain unconfined, Baikenov was arrested at his Almaty apartment by the National Security Committee officers, transported to Astana,

68 “Publication of any details of an official’s private life will lead to imprisonment,” [in Russian] Exclusive, May 27, 2013, [link]
69 Farangis Najibullah and Makpal Mukankyz, “Journalists Express Concern Over Kazakh Data-Protection Law,” RFE/RL, [link]
70 Natalia Marchelova, “Websites are media, or not,” [in Russian] Respublika-kaz, [link]
71 “New rules of journalists’ accreditation adopted in Kazakhstan,” Internews, [link]
72 Gaziza Baituova, “First Prosecution for Internet Hate Speech in Kazakhstan,” Institute War and Peace Reporting, [link]
73 “Kazakh Court Convicts Woman Over Slurs, Calls To Join Russia,” RFE/RL, [link]
and taken into custody for two months. In April 2015, Baikenov was found guilty and sentenced to two years of restriction of freedom. The confiscated devices he had been using to access internet were ordered to be demolished.

In both of these cases, the pages were removed from Facebook, but it is unclear whether they were removed by Facebook following users’ complaints, by law enforcement agencies, or by Shevtsova-Valova and Baikenov themselves.

Abai Yerekenov, a member of the “Protect Kok-Zhailau!” group and active critic of the Almaty city administration on Facebook, was briefly detained on February 19, 2015, as he was heading to the annual public meeting with city mayor, Akhmetzhan Yessimov. Police initially said that they regarded him as a suspect in a robbery, but released him without explanation hours later when the doors to the mayoral event were already closed. Police were documented preventing critics of Yessimov from attending similar meetings in past Freedom on the Net reports.

Valery Surganov, journalist and owner of the political commentary website Insiderman, was sued by a judge in 2014 for alleged defamation and hindrance to justice. In July 2014, the case was closed after a settlement. Surganov admitted that the article was “inadmissibly subjective and contained unverified data.” He apologized for the moral damage, and the judge agreed to drop the charges.

### Surveillance, Privacy, and Anonymity

It is difficult to estimate the scope and depth of government surveillance of online communications in Kazakhstan, though the “system for operational investigative measures” (SORM) system of surveillance implemented by the government is similar to that of other former Soviet republics and allows for deep packet inspection (DPI) of data transmissions. The general public, as well as civil society activists, often underestimate the potential threat of government surveillance and do not always use privacy-enhancing or encryption techniques.

Since early 2011, some anonymizing sites and proxy gates have been blocked in Kazakhstan, apparently without a proper court decision issued against them. In June 2015, the media began reporting that the authorities were going after such tools, citing a court decision dated September 10, 2014 that banned “the functioning of networks and/or means of communication that can be used to circumvent the technical blocking by ISPs.” No liability for users is specified, but in the past, cybercafes were forced to delete or block circumvention tools. Internet users wishing to circumvent censorship often use the traffic compression mode in Opera browsers, and, increasingly, VPNs. The current regulation on public access points bans the use of circumvention tools in cybercafes.

The Tor Project’s official website is intermittently inaccessible from Kazakhstan. It has been blocked

---

79 Olzhas Asuyezov, “Web browser that bypasses big brother a Kazakh hit,” Reuters, April 13, 2010, [http://reut.rs/1LdBYe0](http://reut.rs/1LdBYe0)
Kazakhstan

at various times throughout the reported period, and remained unavailable as of May 2015. It is difficult to verify how far the Tor network itself is affected by blocking, but according to the public records of its use, the number of connections to the service's "relay" nodes from Kazakhstan dropped by about 40 percent in October. The number of users connecting via "bridge relays," which are not listed publicly and are more difficult to block, increased about 800 percent. This pattern often indicates a censorship event.

SIM card registration is required for mobile phone users. In October 2014, all mobile operators received a letter from the Ministry of Investments and Development, asking them to make their client databases compliant with the official standards concerning user registration. Provision of services to unregistered numbers was required to be suspended on December 10, 2014. The government justified this step by the "need to ensure public security." 81

A professional from a private-sector telecom company who spoke on the basis of anonymity stated that the president's administration, the prosecutor general's office, and the National Security Committee have been planning to launch three different content monitoring systems, including software to monitor social networking sites. In the past, the Almaty city administration admitted that it monitors popular social networking sites. 82 Several times, Facebook users who planned to take part in protest actions reported that they had been subject to "preemptive" police visits to their residences to "discuss their Facebook posts" and warn them against going to an unsanctioned gathering. 83 In January 2015, an unauthorized rally in support of the Adam Bol magazine was announced and coordinated via social media, but key participants—including journalists and human rights activists—were detained near their residences as they were heading to the gathering. 84

Kazakhtelecom maintains that its DPI system is used for traffic management and has no access to users' personal data. 85 According to Shavkat Sabirov, president of the Internet Association of Kazakhstan (IAK), the DPI system was installed on the backbone infrastructure in 2010 by the Israeli company Check Point Software Technologies. 86 Leaks of Sabirov's email correspondence released by hackers in January 2015 pointed to even closer ties between the IAK and the prosecutor general's office. In an interview with Ratel.kz, the IAK president confirmed the authenticity of emails, 87 which indicated that the IAK may be involved in handing over personal data (like IP addresses) of online commentators on news sites to prosecutors.

The government places no legal restrictions on anonymity online. However, legislation obliges both ISPs and mobile operators to retain records of users’ online activities, including phone numbers, billing details, IP addresses, browsing history, protocols of data transmission, and other data, via the installation of special software and hardware when necessary. 88 Providers must store user data for two years and grant access within 24 hours to "operative-investigatory bodies," including the Na-

86 As said at the Roundtable "How to make internet safe for children" in Almaty, April 14, 2014.
87 Kalashnikova, "Shavkat Sabirov.
Kazakhstan

Tional Security Committee, secret services, military intelligence, when sanctioned by a prosecutor, or in some cases “by coordination with prosecutor general’s office.”

Additionally, the 2013 law on countering terrorism granted extra powers to the security bodies and obliged mass media (including internet resources) to assist the state bodies involved in counter-terrorism. However, the exact mechanisms of assistance are not specified.

Under the 2011 governmental decree tightening surveillance in cybercafes, owners are obliged to document customers’ IDs before letting them access the internet, install video surveillance equipment and filtering software, and retain data about their online activities and browsing history. This information is to be retained for no less than six months and made readily available to “operative-investigatory bodies.” However, cybercafes are almost extinct in cities, and rarely register ID in practice. The regulation does not apply to public Wi-Fi access points.

Intimidation and Violence

No incidents of intimidation or physical violence against online users have been reported during the coverage period.

Technical Attacks

There were fewer reports of technical attacks against critical internet-based media or government websites than in previous years, though cyberattacks still pose a threat.

On January 26, 2015, the website of the Legal Media Center, a prominent media advocacy NGO, was hacked. The attackers posted irrelevant content on the website and a database of government procurement contracts in the information sphere, the focal point of the NGO’s activity, was rendered inaccessible for users.

Valery Surganov, the owner of the political blog Insiderman, was informed by the hosting provider that his website was taken down by a DDoS attack in March 2015, despite the fact that it was rarely updated and recently changed its critical stance toward the incumbent president, becoming more supportive.

On March 13, 2015, it was reported that Kazakhstan was suing unidentified hackers who broke into government computers and posted confidential emails exchanged between officials and a New York law firm. According to the lawsuit, thousands of messages sent from Gmail accounts belonging to Kazakhstan officials were stolen. The misappropriated emails included some from Marat Beketayev, Kazakhstan’s executive secretary of the Ministry of Justice, and Deputy General Prosecutor Andrey Kravchenko. Some emails were posted on Facebook, according to the complaint.

92 “Rules of rendering internet access services.”
94 Patricia Hurtado, “Kazakhstan Sues Hackers Who Stole,Posted Officials’ E-Mails,” Bloomberg Business, March 13, 2015,
Kazakhstan

The National Computer Emergency Response Team (CERT),95 a state body designed to fight cyberattacks and malware, and to provide information security advice to the government, organizations and individuals, also lists “monitoring and detection of internet resources hosting illegal content” among its objectives.96 This has been a matter of concern to analysts, but currently the CERT website declares that this refers only to technical, not political, content, and that they are not authorized to deal with issues that fall under the authority of law enforcement bodies.97 However, in November 2014, the Kyrgyz website Kloop received a request to take down materials about Kazakh jihadists in Syria (see Blocking and Filtering). The letter was sent to Kloop by a Kazakhstani CERT employee.98

http://bloom.bg/1wHn6n

Kenya

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>28</td>
<td>29</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 43.2 million
Internet Penetration 2014: 43 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: Yes
Press Freedom 2015 Status: Partly Free

Key Developments: June 2014 – May 2015

- Blogging has become an economically viable industry for bloggers who are increasingly sought by Kenyan businesses as a platform for advertising (see Media, Diversity, and Content Manipulation).

- Government officials in Kenya twice turned to the courts to compel intermediaries to take action against defamatory content about them posted online (see Content Removal).

- An unprecedented number of Kenyan bloggers and social media users were arrested and in some cases charged with "misuse of licensed telecommunications equipment" in 2015, mainly for their online commentary criticizing government officials (see Prosecutions and Detentions for Online Content).

- In the context of the fight against terrorism, several developments led to increasing concerns over the government’s surveillance powers (see Surveillance, Privacy, and Anonymity).
Introduction

In 2014-2015, Kenya’s information and communication technologies (ICT) sector continued to be vibrant, characterized by laudable growth due to investments from global ICT companies and the country’s strong environment for innovation. The capital, Nairobi, was ranked in January 2015 as the “most intelligent” city in Africa by the Intelligent Community Forum for the city’s efforts to build “inclusive, prosperous economies on a basis of information and communication technologies.”¹ Nairobi is also the center of the global mobile money revolution, with nearly 60 percent of Kenya’s adult population using mobile money platforms.² Further, Nairobi has become an incubator for local content creators, home to the world-renowned technology community for tech entrepreneurs and programmers, “i-Hub.” Meanwhile, blogging has become an economically viable industry for bloggers who are increasingly sought by Kenyan businesses as a platform for advertising.

Nonetheless, sensitivities around hate speech since the tumultuous 2008 elections and growing terrorist threats have led the government to take steps to limit online freedom of expression and violate user privacy in recent years. In December 2014, the government hurriedly passed the Security Laws (Amendment) Act 2014 with little stakeholder consultation, granting power to national security organs to intercept communications without proper judicial oversight in order to detect, deter, or disrupt terrorist activities. The law was challenged in court in late December, resulting in the suspension of eight controversial provisions in February 2015, including a provision that imposed high fines and a possible jail term for journalists who publish or broadcast images of terror attacks. Nonetheless, the law still contains vaguely worded provisions that may violate freedom of expression.³

Online freedom of expression is also threatened by a provision in the 2013 Kenya Information and Communications Act (KICA) that penalizes the “misuse of licensed telecommunications equipment” for disseminating “offensive” or “annoying” messages, which was frequently used to arrest and prosecute several bloggers and social media users in 2015, mainly for posts that criticized government officials. Officials also applied legal pressure on intermediaries for objectionable content.

Obstacles to Access

Steadily increasing access to the internet was fueled in large part by relatively low-priced mobile services and expanding mobile broadband networks in Kenya. The telecommunication regulator’s murky independence was questioned following irregularities in the board’s appointment process.

Availability and Ease of Access

Information and communication technologies (ICTs) are continuing to spread in Kenya, in no small part due to the government’s commitment to developing the country’s ICT infrastructure as a tool for economic growth. According to available government data from December 2014, the percentage of the population with access to the internet stood at over 64 percent, increasing from 52 percent

¹ Alex Court, “What makes Nairobi Africa’s ‘most intelligent’ city,” CNN, February 10, 2015, http://cnn.it/1CPLrUQ.
³ ARTICLE 19 remains concerned that the provision that criminalizes the adoption or promotion of “extreme belief systems” for the purpose of “facilitating ideologically based violence to advance political, religious or social change” remains on the statute book. Article 19, “Kenya: High Court ruling on security amendment act a victory for free speech,” press release, February 26, 2015, http://bit.ly/1RRjJ3.
Kenya

recorded a year earlier, driven in large part by internet-enabled mobile phones that provide value-added mobile services such as social media, entertainment, mobile money transfer, and lower cost text messaging applications. Data from the International Telecommunications Union (ITU) from 2014, which may not count mobile internet access, estimated a lower penetration rate of 43 percent, up from 39 percent in 2013.

The government reported a figure of over 31 million mobile phone subscriptions in 2014, equating to a mobile phone penetration rate of 80 percent (73 percent according to 2014 ITU data), though many people have more than one subscription with different providers to take advantage of lower prices or expand their geographic coverage, putting the actual number of users much lower. The mobile sector is the predominant provider of data and internet services to Kenyan users, accounting for 99 percent of total internet subscriptions. Penetration for fixed-line broadband subscriptions remained very low at 0.2 percent in 2014.

In November 2014, the government announced a promise to increase access to affordable high speed broadband throughout the country in an effort to lower data transmission costs. In line with the 2013 National Broadband Strategy, Kenya anticipates that the country will have national minimum speeds of 5 Mbps by 2017, compared to current average speeds of 1.4 Mbps. In light of this, different data providers are working towards connecting major urban centers with fiber optic cabling. However, the lack of a regulatory framework to allow for infrastructure sharing has resulted in inefficient duplication in the construction of towers, ducts, and access roads.

Kenya has comparatively low-priced mobile services in Africa, with monthly costs averaging KES 161 (US$1.90) for 30 calls and 100 SMS text messages. Data bundles are available for prepaid mobile customers, while mobile broadband subscriptions on GPRS/EDGE and 3G networks have also continued to increase. The growth in mobile internet subscriptions can be attributed to competitive mobile internet tariffs, special offers and promotions, competition between the various cell phone providers, and the rise in social media use, particularly among the youth population. In 2014, Kenya was ranked by the Alliance for Affordable Internet as the fifth most affordable country in Africa for internet access.
Kenya

While internet penetration continues to increase across the country, there is still a large urban-rural divide in access, with internet use mainly concentrated in Nairobi.\(^{18}\) In addition, large rural areas of the country have not been able to benefit from Kenya’s high-capacity bandwidth in part due to market disparities and weaknesses in last mile connectivity, which is pricey and requires basic infrastructure such as electricity and roads that are often poorly developed in rural areas. This prompted the government to establish the Universal Service Fund (USF) in 2013 to raise KES 1 billion yearly from the industry in order to expand mobile and internet services.\(^{19}\) As of March 2015, the Communications Authority of Kenya reported that the USF had exceeded targets and stood at KES 2.5 billion raised from different telecom companies, with the dominant player Safaricom contributing KES 1.3 billion.\(^{20}\) The funds will be used for the development of communications infrastructure in remote areas where private companies are less likely to invest.

Restrictions on Connectivity

During the year under review, there were no reports of the government controlling the internet infrastructure to limit connectivity. Kenya connects to the international internet via four undersea cables—Seacom, the East Africa Marine System (TEAMS), EASSY, and Lower Indian Ocean Network (LION2)—which has enabled increases in high speed broadband and improved internet speeds over the past several years. License provision of the internet gateway was liberalized in 2004.\(^{21}\)

ICT Market

Kenya’s ICT sector is competitive and comprised of over ten internet service providers (ISPs) and three mobile phone providers. In 2015, Safaricom continued to dominate the market for mobile phone services with a market share of 76 percent for voice services, 93 percent for SMS, 70 percent for mobile data, and 67 percent for mobile money.\(^{22}\) The two other mobile operators—Airtel Networks and Telkom Kenya (Orange)—served the other share of the mobile market. There are no limitations on the number of operators permitted to launch and operate telecommunications infrastructure, with both data carriers and cellular licenses allowed to run domestic fiber networks.\(^{23}\)

Associations such as the Kenyan ISP Association, the Telecommunications Service Providers of Kenya (TESPOK), and the Kenya Cybercafe Owners enable ICT providers to lobby the government for better regulations, lower costs, and increased efforts to improve computer literacy.

Regulatory Bodies

Kenya’s telecommunications sector is regulated under the Kenya Information and Communication

---


\(^{22}\) Communications Authority of Kenya, *Quarterly Sector Statistics Report: First Quarter of the Financial Year (July-Sep 2014).*

Kenya

Amendment Act (KICA) 2013, which established the Communications Authority of Kenya (CA) as the country’s regulator for both broadcast and online media. While KICA explicitly enshrines the independence of the CA, the act was widely criticized for the power it granted to the Cabinet Secretary to appoint the new authority’s board without stakeholder input as well as the presidential appointment of the board’s chairperson. The regulator’s murky independence was questioned in May 2015 when the High Court disbanded the CA’s board after what it determined were irregularities in the appointment process. The Ministry of ICT responded by appealing the decision.

Limits on Content

No websites were blocked during the coverage period, though a number of blogs and social media profiles were targeted for removal. The exponential growth in blogs has created an economically viable industry for bloggers who are increasingly sought by Kenyan businesses as a platform for advertising.

Blocking and Filtering

Kenya does not actively block or filter internet content, and Kenyans have unrestricted access to social networking platforms and communication applications such as Facebook, Twitter, YouTube, and Wordpress, all of which rank among the 20 most popular websites in the country.

However, the Blue Coat PacketShaper appliance—a device that can help control undesirable traffic by filtering application traffic by content category—was detected in Kenya in January 2013, as well as in 18 other countries around the world, including China, Bahrain, and Russia. There has been no further evidence to reveal the extent to which the filtering device has been implemented, though its discovery in Kenya is noteworthy given the government’s increasing concern over the spread of hate speech and inflammatory content via ICTs.

Content Removal

Despite the lack of website blocking in Kenya, a number of blogs and social media profiles were targeted for removal during the coverage period, including the blog and Twitter page of Abraham Mutai in January 2015 following his arrest for his reporting on government corruption (see “Prosecutions and Detentions for Online Activities”). Mutai’s blog and Twitter account were reinstated upon his release on bond. Blogger Robert Alai also had his Twitter account suspended in December 2014 after he allegedly insulted the Kenyan president and publicly shared the personal mobile numbers of
Kenya

government officials, the latter of which was seen as being in line with Twitter’s policy against posting another person’s private and confidential information.\textsuperscript{30}

Intermediaries can be held liable for illegal content, such as copyright and hate speech, though they are not required to actively monitor traffic passing through their networks unless they are made aware of illegal content.\textsuperscript{31} Under the National Cohesion and Integration Act of 2008, which outlaws hate speech, a media enterprise can be fined up to KES 1 million (nearly US$11,000) for publishing “utterances” that can be characterized as hate speech under the law's broad definition.\textsuperscript{32} According to analysis by the Association of Progressive Communications (APC), this provision can be invoked to either block or take down online content.\textsuperscript{33} Issues of intermediary liability are further complicated by the fact that the Kenyan judicial system and media are not fully conversant of legal norms involving the internet.

In recent years, government officials in Kenya have increasingly turned to the courts to compel intermediaries to take action against defamatory content about them posted online. In September 2014, an administrator of a Facebook group page called “Dead Beat Kenya” was issued an injunction under a libel suit, restraining the administrator from publishing information about Kiambu county assembly member, Paul Karungo. Dead Beat Kenya is a Facebook group dedicated to naming and shaming spouses who abdicate parental responsibilities.\textsuperscript{34} The assembly member had sued the Dead Beat Kenya administrator for a defamatory post that claimed he had failed to provide child support for his child.\textsuperscript{35} Karungo also sued the mother of the child who had authored the allegedly defamatory post on Facebook and sought to have all offending posts and associated comments from the Facebook group’s page taken down.\textsuperscript{36}

Another ongoing intermediary liability case began in July 2014 when Cabinet Secretary Anne Waiguru sued Google Kenya and Google Inc. over an April 2014 story she claims defamed her on the Kenyan news and gossip blog, Daily Post, which is hosted on Google's Blogger.com platform.\textsuperscript{37} Ms. Waiguru sued the search engine to obtain the identities of Daily Post’s owners, against whom she sought to take legal action for the defamatory story.\textsuperscript{38} Citing the 2014 European Union Court of Justice case that established the so-called “right to be forgotten” principle in the EU,\textsuperscript{39} she also wanted Google to take down the offensive article from its search engine and remove it permanently from the Daily Post’s website. On its part, Google Kenya argued that it was in no position to take down the offensive article or supply the information sought by Ms. Waiguru given its role as a commercial agent of

\textsuperscript{31} Alice Munyua, Grace Githaiga and Victor Kapiyo, “Intermediary Liability in Kenya,” (research paper, commissioned by Association for Progressive Communication) \url{http://bit.ly/1GOXHDe}.
\textsuperscript{32} Section 62 (1) defines hate speech as “words intended to incite feelings of contempt, hatred, hostility, violence or discrimination against any person, group or community on the basis of ethnicity or race.” Section 62 (2) holds: “A newspaper, radio station or media enterprise that publishes the utterances referred to in subsection (1) commits an offence and shall be liable on conviction to a fine not exceeding one million shillings.” See: National Cohesion and Integration Act, 2008, section 62, accessed September 12, 2014, \url{http://bit.ly/1ZR1dbX}.
\textsuperscript{33} Munyua, Githaiga and Kapiyo, “Intermediary Liability in Kenya.”
\textsuperscript{34} Dead Beat Kenya Updates, Facebook Page, \url{https://goo.gl/LDRpKi}.
\textsuperscript{35} Vincent Agoya, “MCA sues Facebook group Dead Beat Kenya for defamation,” Daily Nation, September 17, 2014, \url{http://bit.ly/1hNCItX}.
\textsuperscript{36} “Confirmed: It was Anne Waiguru who wanted to sleep with Janet Mbugua’s boyfriend Gor Semelango,” Okoo News, April 14, 2014, \url{http://bit.ly/1NkjqYu}.
\textsuperscript{38} Google Spain, Google Inc vs AEPD and Mario Costeja Gonzalez.
Kenya

Google Inc. In December 2014, the Constitutional and Human Rights court ruled that the information brought to court was insufficient as to determine with certainty Google Kenya’s responsibility and if it had been in a position to prevent publication of the offensive material, leaving the case on hold until a further hearing.

Media, Diversity, and Content Manipulation

Kenya’s online information landscape is diverse and vibrant, representing a wide range of issues and viewpoints. There are no state-run online news outlets, and the most popular news websites include the BBC, CNN, and Kenya’s Standard Online and Daily Nation. While print outlets, television, and radio continue to be the main sources of news and information for most Kenyans, all major television stations have live-stream features and use YouTube to rebroadcast news clips and actively engage audiences on Facebook and Twitter.

Bloggers and social media personalities have become highly influential over the past few years, as the increase in fast and affordable internet in major cities and towns across the country has enabled Kenya’s growing class of digitally skilled citizens to become content creators and alternative sources of news and information. According to the Bloggers Association of Kenya (BAKE)—formed in 2011 to support Kenya’s blogging community—there are an estimated 15,000 registered blogs in the country as of mid-2015, covering a diverse range of topics such as fashion, the environment, food, politics, health, and human rights. The exponential growth in blogs has created an economically viable industry for bloggers who are increasingly sought by Kenyan businesses as a platform for advertising.

The government does not impose any economic constraints on online media in Kenya, which has helped online outlets thrive. In recent years, the sale of many print newspapers has been eclipsed by online news sources, a trend which led the president to announce in March 2015 that government advertising would be shifted to digital platforms to cut down on government spending and reliance on newspapers and television stations for advertising. In his directive, the president opined that digital platforms are cheaper and effective given their broad reach.

Individual internet users are generally comfortable expressing themselves openly online, though the use of digital technologies to spread ethnic, racist, and xenophobic commentary continues to pose a serious challenge to freedom of expression in Kenya, particularly during politically contentious periods such as national elections. In this complex debate, and in the absence of a suitable framework to regulate online hate speech, many feel that the emphasis should be on self-regulation by internet users, with the government stepping in when needed to address hate crimes on the internet. Nonetheless, observers worry that self-censorship may rise as the growing number of bloggers and ordinary users targeted by the government for arrest over the past year has led to increasing caution among internet users in criticizing the government.

Digital Activism

The internet continues to grow as an important platform for political debate and mobilization around critical issues in Kenya. Additionally, digital media has revolutionized the ways in which citizens and civil society groups in Kenya network, share information, and effect change.

Kenya has an estimated 700,000 active Twitter users (out of over 2 million total internet users), many of whom frequently take to the social media platform to comment on social and political issues. One instance of successful digital activism took place a few days before the inauguration of Nigerian President Muhammadu Buhari in May 2015, which Kenyan President Kenyatta planned to attend. Social media users expressed outrage when it was leaked that Kenyatta’s trip to Nigeria entailed an 84-person delegation that would cost the taxpayers KES 20 million. The uproar forced the president to cancel his trip and instead send the deputy president.

Another successful social media campaign involved the hashtag #MyDressMyChoice in November 2014, which was sparked by an online video that captured a mob of men assaulting and stripping a Kenyan woman whom they claimed was indecently dressed. The hashtag campaign corresponded with public demonstrations in the streets of Nairobi calling for action against the perpetrators and ultimately resulted in an estimated 90 arrests of individuals suspected of their involvement in the assault.

Violations of User Rights

An unprecedented number of Kenyan bloggers and social media users were targeted for arrest or summoned for questioning in 2014-2015, mainly for their online commentary criticizing government officials. Several developments in 2014 and 2015 led to growing concerns over the government’s surveillance powers and increasing restrictions on anonymity, undertaken in response to the growing threat of terrorism.

Legal Environment

Freedom of expression is enshrined in Article 33 of Kenya’s 2010 constitution and includes the right to seek, receive, or impart information and ideas, while Article 31 provides for the right to privacy. These rights, however, do not extend to propaganda, hate speech, or incitement to violence. Hate speech is penalized under the 2008 National Cohesion and Integration Act, passed in response to widespread ethnic violence that ensued after the 2007 general elections. Individuals found guilty of spreading hate speech, broadly defined, can be fined up to KES 1 million (nearly US$11,000), sentenced to up to three years in prison, or both.

---

47 1 US$ is approximately Kes. 96.
Section 132 of the penal code, which penalizes “undermining the authority of public officers,” also constrains freedom of expression, both online and off.\(^53\) Meanwhile, criminal defamation laws remain on the books, waiting to be repealed or amended to conform to Kenya’s 2010 constitution.

Online expression is specifically targeted under Section 29 of the Kenya Information and Communications Act (KICA) 2013, which penalizes the use of ICTs to disseminate messages deemed to be “grossly offensive” or that cause “annoyance, inconvenience or needless anxiety to another person” with a fine of up to KSH 50,000, three years in prison, or both.\(^54\) Section 29 of KICA was used to arrest and, in some cases, charge an unprecedented number of bloggers and social media users for their online activities in 2015 (see “Prosecutions and Detentions for Online Activities”).

A number of positive laws have been proposed in recent years to protect the rights of Kenyan internet users. The Data Protection Bill 2012, though still in draft form as of mid-2015, aims to regulate the collection, processing, storing, use, and disclosure of information relating to individuals processed through automated or manual means.\(^55\) The 2013 Freedom of Information Bill underwent stakeholder consultation in mid-2013 and awaits further consideration in parliament as of mid-2015.\(^56\) Both bills promise to strengthen internet freedom in Kenya, though the current absence of a strong data protection law threatens citizens’ privacy rights amid rising concerns over unchecked government surveillance (see “Surveillance, Privacy, and Anonymity”).

### Prosecutions and Detentions for Online Activities

An unprecedented number of Kenyan bloggers and social media users were targeted for arrest or summoned for questioning in 2014-2015, mainly for their online commentary criticizing government officials. In previous years, arrests usually involved well-known and controversial blogger Robert Alai, who was arrested in 2012 for tweeting about a government spokesman\(^57\) and again in 2013 for making allegedly false accusations on Twitter.\(^58\)

Alai was arrested once again in December 2014 for insulting the president by calling him an “adolescent president” on Twitter after it emerged that President Kenyatta had proceeded to go watch the Formula One race in Abu Dhabi on the day an Al-Shabaab terror attack had hit Mandera County,\(^59\) killing 28 people on a school bus in November. He was also accused of posting the personal phone numbers of government officials on Twitter.\(^60\) Released on bail in December, Alai still faces the charge of undermining the presidency as of mid-2015.\(^61\) Adding to the ongoing case against him, Alai was arrested yet again in February 2015 for discussing a land-grab controversy in the country on his Facebook wall.\(^62\)

---

A number of other bloggers and social media users were arrested and in some cases prosecuted for the “misuse of licensed telecommunications equipment” under section 29(a) of the 2013 Kenya Information and Communications Act (KICA) during the coverage period.\textsuperscript{63}

- Allan Wadi Okengo, a university student, was arrested in December 2014 and later found guilty of insulting the president and inciting ethnic hatred on his Facebook wall. He was sentenced to two years in prison and fined KES 200,000 (approximately $2,200) in January 2015\textsuperscript{64} and subsequently released on appeal in July 2015.\textsuperscript{65}

- Abraham Mutai, a blogger known for his investigations on corruption, was arrested for posting a blog about corruption and charged with “using a media platform to cause public anxiety” in January 2015. He was released a day later after significant social media attention called for his release.\textsuperscript{66}

- Nancy Mbindala, an intern at the Embu county government office, was arrested in January 2015 for a series of posts she wrote on her Facebook wall from 2013–2014 that allegedly abused a local governor. She was later released and pardoned of all charges after apologizing to the governor.\textsuperscript{67}

- Geoffrey Andare, a web developer, was charged in March 2015 with improper use of ICTs for his Facebook post that accused an employee of a nonprofit educational organization of trading scholarships for sexual favors. Andare used the charge as an opportunity, in partnership with Article 19, to file a petition challenging the constitutionality of section 29 of the KICA, which violates Kenyan citizens’ constitutional right to freedom of expression. The petition had not been heard as of mid-2015.\textsuperscript{68}

**Surveillance, Privacy, and Anonymity**

The Kenyan government has stepped up its surveillance efforts in the past couple of years to deal with the threat of terrorism, which became particularly pronounced following the September 2013 Al-Shabab terrorist attack on the Westgate mall in Nairobi. Several developments in 2014 and 2015 led to growing concerns over the government’s surveillance powers and increasing restrictions on anonymity:

- In February 2014, SIM card registration requirements became more restrictive under the Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations, 2013, which prescribed higher penalties than the previous regulations of up to KES 300,000 (approximately US$3,500) or imprisonment of up to three years for...

\textsuperscript{63} Confirmed! Robert Alai Has Been Arrested,” Kenya Digest (blog), February 5, 2015, \url{http://bit.ly/1M1Cq0y}.

\textsuperscript{64} Other cases include: Boniface Mwangi, “Ph God!! Young Man Arrested for Carrying His Laptop without a Receipt. He Refused to Bribe Police,” Jobs Kenya Hapa, \url{http://bit.ly/1MF0uyB}; Shitemi Khamadi, “Patrick Safari aka ‘Modern Corps’ arrested and charged for ‘annoying tweet’,” Kenya Monitor, July 30, 2015, \url{http://bit.ly/1PcSY8g}.

\textsuperscript{65} “Kenyan jailed for insulting President Uhuru Kenyatta,” BBC, January 2, 2015, \url{http://bbc.in/1xoMrMf}.


\textsuperscript{67} “#FreeSpeechStories: Arrested for a tweet.”

failure to abide by the registration requirements. The new regulations also granted the communications regulator with access to service providers’ offices and records without a court order, raising concerns over the blatant lack of judicial oversight.

- In November 2014, the government contracted Kenya’s largest mobile service provider Safaricom to develop a security communication and surveillance system, known as the National Police Integrated Public Safety Communication and Surveillance Project (IPSCSS), to boost the capacity of the country’s national security agencies to fight terrorism. Among the project’s various components, the surveillance system will connect 195 police stations with high speed internet, and develop a 4G LTE network for the police with 80 base stations. The system is expected to be completed in 2016. Stakeholders have raised numerous concerns over the Safaricom contract with the government, including doubts about the integrity of the system, the company’s independence, and the apparent conflict of interest. There are also worries that, in the absence of strong data protection standards, law enforcement agencies will be able to freely access Safaricom’s database of over 20 million subscribers to match with a facial recognition system also being developed under the surveillance project.

- In December 2014, the government hurriedly passed the Security Laws (Amendment) Act 2014 with little stakeholder consultation, granting power to national security organs to intercept communication in the interest of detecting, deterring, or disrupting terrorist activities without proper judicial oversight. The law was challenged in court in late December, resulting in the suspension of eight controversial provisions in February 2015, including a provision that imposed high fines and a possible jail term for journalists who publish or broadcast images of terror attacks. Nonetheless, the law still contains vaguely worded provisions that may violate freedom of expression.

- In July 2015, Wikileaks published leaked emails from the Italian surveillance company Hacking Team, which revealed efforts by Kenya’s National Intelligence Service (NIS) to acquire Hacking Team’s sophisticated spyware known as Remote Control Systems (RCS) in April and May 2015. The leaked emails also included a request by a government representative to

---

70 Section 13. “A licensee shall grant the Commission’s officers access to its systems, premises, facilities, files, records and other data to enable the Commission inspect such systems, premises, facilities, files, records and other data for compliance with the Act and these Regulations.” The Kenya Information and Communications (Amendment) Act, 2013, http://bit.ly/1M1zTDB.
76 According to ARTICLE 19, the provision that criminalises the adoption or promotion of “extreme belief systems” for the purpose of “facilitating ideologically based violence to advance political, religious or social change” remains on the statute book. Article 19, “Kenya: High Court ruling on security amendment act a victory for free speech,” press release, February 26, 2015, http://bit.ly/1RRijJ3.
take down controversial blogger Robert Alai’s anti-corruption news website, Kahawa Tungu, as “proof of concept” of Hacking Team’s capabilities.\textsuperscript{78} Later emails from July 2015 revealed that Hacking Team ultimately rejected the government’s requests out of concerns over the Kenyan government’s intentions.\textsuperscript{79}

**Intimidation and Violence**

Violence against online journalists and ordinary internet users is not common in Kenya, though a few incidents over the past couple of years have created cause for concern. As of mid-2015, the chief editor of the controversial news blog *Jackal News*, Dickson Bogonko Bosire, remained missing after he mysteriously disappeared in September 2013.\textsuperscript{80} Bosire had periodically experienced threats in response to his blog’s coverage of corruption investigations and scandals, which had led him to go into hiding or flee Nairobi on several occasions.

In June 2015, Twitter activist Wanjeri Nderi was assaulted at a shopping mall by an unidentified individual who had reportedly demanded her to “stop making noise” before attacking her. Known for her Twitter posts about corruption and injustice in Kenya, Nderi and her supporters believe she was targeted for her frequent criticisms of the government.\textsuperscript{81}

**Technical Attacks**

There were no politically motivated cases of technical violence against civil society, independent news, or opposition websites during the coverage period, though leaked emails published by Wikileaks in June 2015 revealed the government’s intentions to launch a technical attack against blogger Robert Alai’s anti-corruption news website in April 2015 (see “Surveillance, Privacy, and Anonymity”).

\textsuperscript{78} “Italians reject bid to close Kahawa Tungu,” *Daily Nation*, July 12, 2015, \url{http://bit.ly/1PtYTnw}.

\textsuperscript{79} Daniel Finnan, “Kenyan government asked Hacking Team to attack dissident website,” *Radio France Internationale*, July 17, 2015, \url{http://rfi.my/1Kkbq4V}.

\textsuperscript{80} Ndesanjo Macha, “Kenyan Blogger Bogonko Bosire is Still Missing, Nearly Two Years After His Disappearance,” *Global Voices Advocacy*, June 18, 2015, \url{http://bit.ly/1W0X03b}.

Kyrgyzstan

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>Partly Free</td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>12</td>
<td>11</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>34</td>
<td>35</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- On June 30, 2014, the government adopted a resolution with new instructions for internet service providers (ISPs) and mobile service providers to update their systems to the latest version of System for Operational-Investigative (SORM) technology. These instructions included requirements for service providers to store the data of their subscribers for up to three years and allow the authorities direct, real-time access to communications networks (see Surveillance, Privacy, and Anonymity).

- On October 29, 2014, the first criminal proceeding based on the law prohibiting the "knowingly false messages about the commission of crimes" was initiated against journalist Dayirbek Orunbekov, for an online article accusing the transitional government in 2010 with responsibility for the victims of ethnic violence. The court dismissed the case based on a lack of evidence; however, the prosecutor general subsequently filed a new charge against Orunbekov for defamation (see Prosecutions and Detentions for Online Activities).
Kyrgyzstan

Introduction

The environment for internet freedom in Kyrgyzstan has improved in recent years, with fewer restrictions since the overthrow of President Kurmanbek Bakiev’s regime in 2010. Despite improvements, internet access remains limited primarily to urban areas, and a number of legal and technical restrictions on online content continue to inhibit internet users. Additionally, increasing requirements for ISPs to implement surveillance technology and a rise in the severity of prosecutions for online content have counteracted improvements in access, causing a slight decline in internet freedom over the past year.

In May 2014, the president signed an amendment to the criminal code introducing criminal liability for distributing information that includes deliberately false accusations of committing a crime, leading to increased concerns about the potential impact of this law on self-censorship in the media. Legislation was passed in February 2014 requiring the immediate registration of SIM cards as a way of legally regulating the relationships between consumers and service providers; however, this regulation also limits the ability of citizens to use information and communications technologies (ICTs) anonymously.

Obstacles to Access

Internet access in Kyrgyzstan is relatively limited, with an internet penetration rate of just 28 percent, although the introduction of unlimited plans by mobile operators and the development of 4G services is improving access. There is still a digital divide between urban and rural areas, as telecommunication companies have fewer incentives to expand services and infrastructure outside of the main cities. The state-owned telecommunications company, KyrgyzTelecom, controls the majority of the market for internet access, with a market share of 78 percent.

Availability and Ease of Access

Access to the internet in Kyrgyzstan continues to expand, though the percentage of the population with internet access is still low by global standards. Internet penetration rates reported by the International Telecommunication Union (ITU), Kyrgyzstan’s State Communication Agency (SCA), and independent research groups vary. According to the ITU, the internet penetration rate in 2014 reached 28 percent, compared to 23 percent in 2013 and just 16 percent in 2009. In contrast, the SCA reported that in 2014 there were over four million active internet users in Kyrgyzstan, or approximately 70 percent of population.

Similar to the ITU report, research conducted in a USAID-funded survey in 2013 by the M-Vector Consulting Agency indicated that about 28 percent of the population was using the internet, with 64 percent of users in urban areas and 36 percent of users in rural areas. Internet users in Bishkek account for 41 percent of all users, while in four of the seven regions, users account for less than 5 percent the total. The majority of respondents—77 percent—mentioned using mobile internet, while

Kyrgyzstan

29 percent reported using the internet at home. Cybercafes have become less popular due to the growing popularity of mobile internet and the spread of broadband infrastructure. The average connection speed in 2014 was 2.7 Mbps.\(^4\)

Fixed-broadband access, via either fiber-optic cables or DSL, is accessible mainly in Bishkek, with broadband in the provinces provided only by the state-run internet service provider KyrgyzTelecom. Broadband speeds range from 24 Mbps for DSL to 100 Mbps for the FTTx (fiber to the x) network, which is well-developed in Bishkek. The government has launched a CDMA 450 mobile telephone and broadband network to expand telecom infrastructure into more rural areas, though it has only become partially active. CDMA 450 phones have become popular in rural areas with more than 30,000 subscribers as of November 2011.

Mobile phone penetration is significantly higher than internet penetration in Kyrgyzstan, with a penetration rate of nearly 128 percent as of the end of 2014, according to the SCA (ITU statistics report a mobile phone penetration rate of 134 percent for 2014).\(^5\) Mobile phone companies claim that their networks cover 90 percent of the populated territory in the country, thus extending the possibility of internet use for most people as mobile web access expands. At the end of 2010, Beeline (one of the largest mobile phone carriers) launched a 3G network that currently covers the entire country. In January 2012, another large firm, Megacom, launched its own 3G network in Bishkek, which by the end of 2013 reportedly covered more than 50 percent of the populated territory of Kyrgyzstan.\(^7\) Saima Telecom has launched a 4G network covering Bishkek and some suburbs. In May 2014, GSM operator NurTelecom (under the brand O!) launched a 4G LTE network covering Bishkek and some surrounding areas,\(^8\) while in April 2015, “Megaline,” one of the biggest FTTH ISPs, launched an LTE network in test mode.

In recent years, the price for internet has decreased and has become more affordable for much of the population, though primarily in the capital where the infrastructure is well-developed and there is greater competition among providers. Prices for 3 Mbps access (the minimal bandwidth offered by many operators) in the capital range from US$15 to $45 per month. The maximum speed available for many customers is 10 Mbps, at a price of about US$70 per month, though not all operators provide access at such speeds. KyrgyzTelecom traditionally has the highest rates for internet access and is the only provider available in most rural areas. An internet connection of 128 Kbps for rural inhabitants in some regions cost around US$14 per month in 2015. Nevertheless, in February 2015, KyrgyzTelecom increased the minimum bandwidth up to 512 kbps without increasing the price. At the same time, KyrgyzTelecom has deployed 52 Wi-Fi hotspots in 16 different locations throughout Kyrgyzstan with free access up to 256 Kbps.

The development of mobile networks provides an alternative to fixed broadband access. The cheapest unlimited data plan at Beeline provides 4 GB of data per month at maximum speeds of 28.8 Mbps, with tariffs of US$4 per GB after reaching the data threshold, and with free access to the

---

\(^4\) M-vector Consulting Agency, Иследование поведения и восприятия медиа аудитории 2012 г. (3-я волна) [Media Consumption & Consumer Perceptions Baseline Survey 2012 (2nd Wave)].
Kyrgyzstan

social network platforms Facebook and Odnoklassniki. This plan costs around US$8 per month. Megacom offers similar options, with monthly 2 GB packages costing around US$10. By comparison, in 2015 the average monthly wage was KGS 12,159 (US$195). In May 2014, the third GSM operator, NurTelecom (operating under the O! brand), became the first mobile operator to launch a 4G network, with speeds up to 150 Mbps.

Restrictions on Connectivity

ISPs in Kyrgyzstan are not required to use government-owned channels to connect to the international internet and can establish their own. In 2010, the state-owned ISP KyrgyzTelecom completed the construction of a fiber-optic cable connection to China, but it has yet to begin functioning as of 2015. Currently, three of Kyrgyzstan’s four first-tier ISPs are linked to the international internet via Kazakhstan and its state-run provider KazakhTelecom; the fourth connects through Russia. In the past, the blogging platform LiveJournal, which was blocked in Kazakhstan, was also accidentally blocked for some internet users in Kyrgyzstan, though as of 2015 this problem appears to have been resolved. The government of Kyrgyzstan does not currently place restrictions on any social media platforms or communication applications.

Fixed-line internet service providers impose different fees for accessing domestic versus international content. All fixed-line operators charge about 10 times less in fees (or do not charge fees at all) for domestic traffic compared to international traffic, due to connections through the local IXP, funded by Soros Foundation in 2000 and currently maintained and owned by Association of Communications Operators, which facilitates the movement of traffic among domestic ISPs. Mobile phone operators do not make this distinction in their data plans and charge the same amount for accessing information, regardless of where it is hosted.

ICT Market

Kyrgyzstan’s telecommunications sector is relatively liberalized and competitive compared to that of other countries in the region; however, the state-owned KyrgyzTelecom is still the largest ISP with a market share of about 78 percent. The other three first-tier ISPs (Elcat, Megaline, and Saima Telecom) are privately owned. The largest among them is Megaline, which provides broadband service in Bishkek, the capital city.

There are seven mobile phone operators providing voice and data services via a variety of technical standards. The two largest competitors, with nearly equal market share, are Megacom and Beeline. Megacom was nationalized in 2010 amid the political upheaval. There are 12 companies with fre-
quencies for deploying 4G networks, but only four of them have begun to use the frequencies for this purpose due to the large investment required in the first stage of deployment.\(^\text{13}\)

In November 2013, the Bishkek inter-district court declared the CDMA network mobile provider Aktel (Fonex) bankrupt. Currently, a special administrator from the government is assigned to deal with the company’s affairs.\(^\text{14}\) At the same time, the director of SCA stated that Aktel’s liquidation will likely have very little effect on the telecommunication market, given that the subscriber base of Aktel is very low compared with other operators (about 27,000 customers). Nevertheless, the director of the Association of Communication Operators pointed out that the loss of Aktel as a mobile phone provider will affect those who need confidentiality in mobile calls, since CDMA provides higher security standards for voice calls.\(^\text{15}\)

### Regulatory Bodies

The main body regulating the ICT industry, including radio spectrum allocation, is the State Communication Agency (SCA), a government body with a director and 137 members. The director and two deputies are appointed by the prime minister.\(^\text{16}\) Some facets of the agency’s work have been criticized, such as the inefficient and non-transparent allocation of radio frequencies and restrictions on wireless mesh networks. Another problematic issue has been the requirement that communication devices (including computers, modems, and wireless access points) be locally certified by the SCA. While this requirement is not systematically enforced, its selective application could serve as an instrument of political pressure and a pretext for authorities to seize “uncertified” property, though this has not yet occurred.

### Limits on Content

Although the government has taken efforts to censor certain content on the internet, in general there are fewer restrictions placed on material that is available online. This may be because television remains by far the dominant medium through which citizens obtain information about their country, and thus censorship efforts have focused on broadcast media.\(^\text{17}\) There have been several incidents of government entities ordering the blocking or deletion of online content in the past, though there were fewer cases over the past year.

### Blocking and Filtering

Many social media outlets such as YouTube, Facebook, and Twitter are freely available. In previous

\(^{13}\) “In Kyrgyzstan, of the 12 companies, only 4 deploying WiMax and LTE networks,” GIP, December 5, 2012, [http://bit.ly/1G1UFk1](http://bit.ly/1G1UFk1).


\(^{16}\) “Regulation on the State Telecommunication Agency under the government of Kyrgyz Republic,” passed by a Resolution of the government of KR № 124, as of February 20, 2012.


www.freedomhouse.org
years, content that was blocked in other countries, through which ISPs in Kyrgyzstan were connected, was also blocked for internet users in Kyrgyzstan. LiveJournal used to be blocked due to this upstream filtering, but it is now available.

On November 24, 2014, the independent online news outlet Kloop.kg reposted a clip of a video originally published by the DailyMail showing children from Kazakhstan training in camps run by the so-called Islamic State. On the same day, the editorial staff received an email from CERT under the Ministry of Communication and Information of Kazakhstan with a request to remove this material, stating that it violates Kazakhstan’s laws; Kloop.kg refused to remove the article, after which the authorities in Kazakhstan blocked the website. On December 10, the SCA sent a notice to all ISPs in Kyrgyzstan to block access to the article within two days. Within five days, access to the site was blocked from the state-owned Kyrgyztelecom and two of the biggest mobile operators, Beeline and Megacom. The SCA also apparently instructed Prohost, the hosting provider for Kloop.kg, to disconnect service to the entire site if the content was not removed. The SCA stated that the order was sent following a request from the Prosecutor General’s office. Later, however, the SCA announced that they had withdrawn the order to block the article, and the access to the site was restored.

On May 13, 2013, the parliament passed amendments to the law “On Counteraction to Extremist Activities,” originally passed in 2005, which allow the government to order the blocking of websites hosted outside the country if the government recognizes the content as “extremist” (previous legislation for blocking extremist content was based on where the website was hosted, rather than from where it could be accessed). These amendments gave rise to criticism from parliamentarians who noted that in order to make the amendments consistent with other legislation, online content should be included in the category of mass media, a proposal which parliamentarians have raised a number of times and which would give the government greater control over online content. At the same time, these amendments were intended to make the process for blocking websites more transparent, since they oblige corresponding bodies to publish the list of blocked resources on their official sites. As of May 2015, no list of blocked sites has been created.

According to the legal requirements in place under the 2005 statute “On Counteraction to Extremist Activities,” originally passed in 2005, which allow the government to order the blocking of websites hosted outside the country if the government recognizes the content as “extremist” (previous legislation for blocking extremist content was based on where the website was hosted, rather than from where it could be accessed). These amendments gave rise to criticism from parliamentarians who noted that in order to make the amendments consistent with other legislation, online content should be included in the category of mass media, a proposal which parliamentarians have raised a number of times and which would give the government greater control over online content. At the same time, these amendments were intended to make the process for blocking websites more transparent, since they oblige corresponding bodies to publish the list of blocked resources on their official sites. As of May 2015, no list of blocked sites has been created.

According to the legal requirements in place under the 2005 statute “On Counteraction to Extremist Activities,” originally passed in 2005, which allow the government to order the blocking of websites hosted outside the country if the government recognizes the content as “extremist” (previous legislation for blocking extremist content was based on where the website was hosted, rather than from where it could be accessed). These amendments gave rise to criticism from parliamentarians who noted that in order to make the amendments consistent with other legislation, online content should be included in the category of mass media, a proposal which parliamentarians have raised a number of times and which would give the government greater control over online content. At the same time, these amendments were intended to make the process for blocking websites more transparent, since they oblige corresponding bodies to publish the list of blocked resources on their official sites. As of May 2015, no list of blocked sites has been created.

---

Activities, the procedure by which a website can be blocked must first begin with a request to the prosecutor. After the request is issued, a review committee must be assembled consisting of representatives from different organizations (linguistic, religious, legal, and so forth) that can confirm the extremist nature of the site. However, members of the committee are appointed by the government, calling into question the committee’s independence and level of objectivity. Once confirmation is granted, a court issues a judicial decision to block the website. However, the process by which state authorities block online content has been inconsistent.

The government has also sought to restrict access to terrorism-related content. By the end of 2014, approximately 25 sites were recognized by the courts as extremist or as inciting national or religious hatred. According to the decision of the court, these sites must be blocked within the territory of Kyrgyzstan. However, the blocking is not consistent: not all sites are blocked and the blocking varies by service provider. According to last amendments to the statute on counteraction to extremist activities, the ministry of justice is required to publish the list of blocked sites, but they have not done so as of May 2015.

In February 2015, the State Committee on National Security proposed to implement a procedure through which websites could be blocked and registration licenses could be withdrawn without a court order. Originally, the committee proposed making amendments to the law “On Counteraction to Extremist Activities,” which would allow the State Committee of National Security to send a request to the SCA to block certain extremist content, without a court order, and the SCA would forward the order to all ISPs. Civil society representatives included in the group protested, referring to the section of the constitution which states that human rights cannot be restricted with “sublegal acts” and proposed not to introduce extra-judicial blocking but to use existing “special” court procedures that oblige courts to make blocking decisions within short period of time (3-5 days). The debates over these potential amendments were still in progress as of May 2015.

The independent Central Asian news website Fergana News has been periodically blocked within Kyrgyzstan. In June 2011, the parliament passed a resolution instructing the government to block the news website based on charges that its content could incite national strife. In February 2012, the SCA sent letters to all ISPs delineating the requirement to block the news website. However, by April 2012, only KyrgyzTelecom had implemented the blocking. On November 19, 2012, the human rights defender organization “Partner Group Precedent,” representing Fergana News, filed a lawsuit against the SCA claiming that the ban on the news site violated the right to freedom of expression. During the court hearings, the SCA representative stated that their letter to ISPs requiring them to take measures on blocking Fergana News was of a voluntary nature and that ISPs were not forced to

---

28 Representatives of the 10th department explained the procedure to the author in a private interview in December 2011.
Kyrgyzstan

block the website.34 In April 2013, the SCA sent official letters to ISPs in Kyrgyzstan confirming that they were not required to block the site. Subsequently, all ISPs—including the state one, Kyrgyz-Telecom—unblocked the site, though the legal status of the original parliamentary resolution is still unclear.35

Content Removal

There were no cases in which the government forced the removal of content online – in most cases, content that the government deems illegal is hosted on servers outside of Kyrgyzstan, so ISPs resort to blocking the content since they cannot require that the host providers remove it.

Media, Diversity, and Content Manipulation

Currently there are no specific economic restrictions imposed by the government that negatively impact users’ ability to publish content online, or that restrict online media outlets’ ability to remain financially sustainable. At the same time, the Kyrgyz blogosphere is not well-developed. There are several popular blog-hosting platforms in Kyrgyzstan (such as Namba.kg, Kloop.kg, Diesel.elcat.kg, and Taboo.kg), but most blogs focus on entertainment, reprint reports from other news agencies, or simply contain a blogger’s personal thoughts on different issues.

There are no particularly popular blogs specifically devoted to political or social issues. Most blogs are in Russian, though some are in the Kyrgyz language, but the latter are not as popular as the former. The internet in general has become an important source of alternative information for users, but since it is primarily the wealthier segments of the population who can afford to consistently access the internet, these are the main participants in online communities.

Self-censorship exists online to a certain degree, primarily as a result of government restrictions against the incitement of national hatred. All posts on forums are strictly moderated to limit this type of content, and online journalists and bloggers generally try to avoid issues concerning ethnic relations. Amendments to the criminal code signed by the president in May 2014, which introduced criminal penalties of up to three years in prison for disseminating false accusations of the commission of crimes, may also cause an increase in self-censorship among bloggers and investigative journalists, though it remains to be seen how these amendments will be applied in the online sphere.

Online platforms such as forums and social networks are actively used for manipulating public opinion, usually by trolls hired by different political actors to influence discussions and express favorable views. Reportedly, the compensation of a troll for one campaign can be anywhere from US$200–700.

Digital Activism

Digital activism efforts remain limited in Kyrgyzstan. Perhaps the most successful online mobilization campaign of the past few years came in 2012 in response to the proposed legislation titled “On protection of children from information threatening to their health and development.” This proposal provoked public outrage, and in an effort to bring attention to the issue, many of the largest ISPs

35 “Kyrgyzstan: News Site Unblocked, Yet Still Illegal.”
and content providers placed banners over their sites with slogans such as: “ATTENTION! This site can be closed. Get to know details and vote against.” The proposal also sparked the internet movement Kyrnet.kg, which conducted advocacy initiatives against the act. Within two months, the site had collected approximately 12,000 votes against the act. Furthermore, in a September 2012 meeting with a group of parliamentarians, representatives of Kyrnet.kg showed the results of the online vote and explained the act’s shortcomings. The parliamentarians agreed that the act needed further elaboration and promised to arrange an extended meeting with all of the parliamentarians who initiated the law for further discussion.36

Violations of User Rights

While there have been few prosecutions for political or social content posted online in the past, in October 2014, journalist Dayirbek Orunbekov was charged for “knowingly disseminating false information regarding the commission of crimes” for writing an article online accusing the transitional government in 2010 of being responsible for the victims of the ethnic clashes in southern Kyrgyzstan. The court dropped the case due to a lack of evidence, though the Prosecutor General subsequently opened a defamation case against the journalist. In addition, the government’s capacity for surveillance of ICTs increased with a regulation requiring upgrades to SORM-3 technology, which instructs service providers to install black boxes on their networks, allowing intelligence agencies unfettered access without a court order.

Legal Environment

The rights to freedom of speech and freedom of expression are legally protected in the new constitution that was approved by referendum in June 2010, and which strengthens the power of the country’s parliament vis-à-vis the president. Article 31 of the constitution guarantees the right to freedom of thought, expression, speech, and press. Article 29 provides constitutional protections over privacy, including private correspondence (by phone, mail, electronics, or other methods), and forbids the collection or dissemination of confidential information without an individual’s consent. Nevertheless, the judiciary is not independent and remains dominated by the executive branch. Corruption among judges, who are generally underpaid, is also widespread, hindering the fairness of decisions in freedom of expression cases as well as others.

In July 2011, the government decriminalized libel to bring legislation in line with the new constitution. Nevertheless, “insult” remains a criminal offense and is punishable by a fine. Officials have long used libel charges to stifle critical media but have not applied these laws against bloggers to date.37 The criminal code contains several provisions (Articles 299 and 299-1) that prohibit “inciting national, racial, religious or inter-regional hostility.” In some cases, the government has sought to apply these provisions in a bid to restrict nonviolent political speech as well.

On May 17, 2014, the president signed an amendment to the criminal code that criminalizes the dissemination of “knowingly false messages about the commission of crimes,” with the stated goal of preventing individuals from making such accusations for political reasons or to damage someone’s

Kyrgyzstan

reputation. The amendment includes fines and sentences of up to three years in prison. Detracting from the progress made through the decriminalization of libel, this amendment could potentially have a chilling effect on online journalists and bloggers, given that criminal penalties can now be levied for such content and that it is unclear exactly how the law will be interpreted. On May 28, 2014, the Association of NGOs and NCOs (noncommercial organizations) of Kyrgyzstan filed a suit with the Constitutional Chamber of the Supreme Court of Kyrgyz Republic, asking the court to recognize the law as contradictory to the Constitution of the Kyrgyz Republic; however, in a decision issued on January 14, 2015, the Court recognized the amendment as constitutional.40

Over the past few years, members of parliament have proposed laws similar to ones passed in Russia that restrict civil liberties broadly, and could have implications for freedom of expression as well. One of these was an initiative that was almost identical to a law passed in Russia obliging NGOs receiving financing from international organizations to register as foreign agents. A draft of the bill was proposed in September 2013 by two deputies in Kyrgyzstan, one of whom is a former ombudsman. Given the vague definitions in the law, critics worried that all forms of civil activities could fall under this law and that NGOs could be shut down without a court decision.41 This initiative was widely debated and several international organizations expressed concern about its potential effects on freedom of expression and assembly.42 On May 26, 2014, the bill was introduced in parliament, and on March 10, 2015 it passed a first reading.43 As of May 2015, the bill was still under review in parliament and had not yet been passed.

In February 2014, some members of parliament submitted a draft of an anti-gay “propaganda” law, similar to the law passed in Russia, which includes criminal and administrative penalties for “propaganda of non-traditional sexual relationships.” The draft received substantial criticism and was withdrawn; however, it was submitted again in May 2014 and in October it passed first readings.44 The draft law includes penalties of fines or imprisonment up to one year for forming positive images of non-traditional sexual relationships through mass media or on the internet. The draft was heavily criticized by civil society and international organizations as discriminatory, and a petition signed by 74 international and local organizations was sent to the president and the relevant committees in parliament in an effort to prevent the legislation from moving forward. As of May 2015, the bill had passed first and second readings, but was still awaiting a third and final reading before being sent to the president.

All traditional media outlets must register with the government. In June 2011, the Prosecutor General’s office proposed amending the statute that regulates mass media45 to include online news

42 ARTICLE 19 and PEN International, “Joint Submission to the UN Universal Periodic Review of Kyrgyzstan.”
44 “Профильный комитет поддержал законопроект об иностранных агентах.”
websites as a form of mass media, requiring them to have a license and to operate with the same responsibilities as traditional media outlets. In January 2012, an expert from the Government Office seconded the recommendation; however, it remains unclear whether online media are to be treated the same under the law as traditional news media outlets.

**Prosecutions and Detentions for Online Activities**

On October 29, 2014, the first criminal proceeding based on the law prohibiting the “knowingly false messages about the commission of crimes” was initiated against journalist Dayirbek Orunbekov, an editor for the online news agency Maalymat.kg. Orunbekov was accused of knowingly disseminating false information about the commission of crimes in his article where he accused members of the transitional government of being responsible for the violent ethnic clashes in 2010 in the south of Kyrgyzstan. The accusation was initiated by the Prosecutor General’s office, rather than through a claim from the injured party, and Constitutional Chamber decided that a journalist could not be accused of this crime based on this article. On April 16, 2015, the case was dismissed due to absence of *corpus delicti* (concrete evidence of the crime), but the next day the Prosecutor General filed a new defamation suit, seeking KGS 1 million (approximately US$ 15,000) in compensation for damage to the honor and dignity of the president. As of May 2015, this case was still pending.

In February 2012, independent journalist and blogger Vladimir Farafonov was charged with inciting national hatred based on his publications on News-Asia.ru, Centrasia.ru and Parus.kg. Farafonov had written a series of articles that were critical of Kyrgyz politics and which examined the potential effects of the 2011 presidential election on the country’s minority populations. The charge was based on the opinion of a commission convened by the security service, but given the fact that the commission was composed of only legal and political experts, Farafonov asked for Russian philology experts to review the case. These experts expressed their opinion that Farafonov had used language that was tough and sometimes tactless, but not extremist. The prosecution had asked for a sentence of 8 years in jail for Farafonov; however, the judge decided to reduce the sentence to a fine of KGS 50,000 (approximately US$1,000). The case became widely known and provoked a wave of indignation from journalists, as there were many cases of similarly tactless expressions by other journalists.

---

52 "Журналист Владимир Фарафонов обвиняется в разжигании межнациональной розни!" [The journalist Vladimir Farafonov is accused in national hatred incitement!] Polit, February 24, 2012, [http://polit.kg/newskg/310](http://polit.kg/newskg/310).
53 "Кыргызстан: После митинга в защиту В.Фарафонова в посольство РФ переданы обращения А.Князева, У.Бабакулова и российских соотечественников," [Kyrgyzstan: After rally in support of V. Farafonov, petitions of A.Knyazev, U. Babakulov and..."
Kyrgyzstan

authors in Kyrgyz language media outlets who received no punishment, indicating that the government applies laws selectively.

Surveillance, Privacy, and Anonymity

Like many former Soviet states, Kyrgyzstan maintains and updates its surveillance technology in line with Russia’s practices. Kyrgyzstan’s surveillance network is modeled after Russian System for Operational-Investigative Activities (SORM) technology, and in August 2012, Kyrgyzstan updated its surveillance network to be on the same level as current Russian interception systems.54

On June 30, 2014, the government adopted a resolution with new instructions for ISPs and mobile service providers to update their systems to the latest version of SORM technology. These instructions included requirements for service providers to store the data of their subscribers for up to three years, and to allow the authorities direct, real-time access to communications networks. Service providers are also required to purchase and update their equipment, at their own expense, to ensure compliance with the new SORM system. While there was evidence to suggest this kind of abuse of surveillance in the past, these new regulations effectively codify the potential for mass surveillance without judicial oversight.

In 2010 and 2011, there were several scandals that revealed the abuse of equipment used for intercepting communications. A subsequent study from June 2011 by the non-profit Civil Initiative on Internet Policy (CIIP) analyzed the legislative framework surrounding interception and its enforcement. It concluded that there were many gaps in the law that enabled interception equipment to be used, and even abused, without sufficient oversight.55 In April 2011, the parliament passed a decision to switch off all interception equipment deployed on the premises of mobile phone operators.56 However, according to reports from September 2011 by members of parliament, the equipment continues to function.57

Since February 2012, the CIIP, together with the Kyrgyz State Committee on National Security and several human rights organizations, have been working on amendments to the statute on the Conduct of Investigations—the body responsible for regulating these issues—that would clarify the circumstances surrounding the use of interception and provide a more adequate legal framework.

There are currently no strict restrictions on anonymous communication on the internet in Kyrgyzstan. Websites do not need to register, encryption software is freely available, and real-name registration is not required to post content online. However, on February 17, 2014, the government issued a new regulation requiring mobile operators to sell new SIM cards only after they have been registered

---

Kyrgyzstan

(previously, SIM cards could be registered within one year of purchase). This new regulation came into force on March 8, 2014, making it more difficult for individuals to use ICT tools anonymously.58

Intimidation and Violence

In general, there is not a significant level of violence or harassment against ICT users in Kyrgyzstan, though there have been some isolated incidents related to online activities this year and in the past. In January 2015, online journalist Bulat Satarkulov was attacked shortly after covering a potentially controversial incident at the international airport. Activist and opposition member Adil Turdukulov had been stopped by the border guard service and was prevented from leaving the country on his way to the United States, under charges claiming that he owed US$600 in debt to private companies. Turdukulov had been scheduled to travel to the United States as part of a delegation of civil society activists and representatives of the Kyrgyz government.59 The next day, Satarkulov, who had filmed the incident, was attacked near his home as he was returning from the airport. The attackers beat him and took away his camera. However, it was not confirmed whether the incident was connected to Satarkulov's coverage of the event.60

In 2014, there were several attacks on journalists, though it is unclear whether the attacks were related to the individuals' reporting. In February 2014, a youth group participating in a rally against LGBT people burned a photo of Ilya Lukash and called him a "destroyer of family values." Lukash is an active blogger and an advocate for human rights of LGBT people; he has also made statements against Kyrgyzstan joining the Eurasian Customs Union and protested in solidarity with the Ukrainian "Euromaidan" demonstrations. Following this incident, Lukash wrote on his Facebook page that he had been forced to leave Kyrgyzstan because of increasing pressure and harassment.

Technical Attacks

Instances of politically motivated cyberattacks are generally rare, including in the run-up to the 2011 presidential elections, but they do occur. In 2005, the OpenNet Initiative recorded the extensive use of distributed denial-of-service (DDoS) attacks against opposition and news websites, demonstrating a precedent for such attacks.61 In September 2011, there was one incident of hackers defacing Kabar.kg, the online government news agency website, but this did not significantly obstruct the agency's work. In March 2012, the social entertainment resource Namba.kg experienced a DDoS attack that was apparently part of an extortion attempt.62 In the same month, the news agency Vesti.kg also reported a DDoS attack on its site, presumably because they had been republishing articles from Fergana News, though the motive remains unconfirmed.

62 As reported by the blog at: "Why Namba did not work over the weekend," Namba (blog), http://blogs.namba.kg/post.php?id=116481.
Kyrgyzstan

During 2012 there were several incidents of cyberattacks on government sites. The sites of the ministry of defense (Mil.kg), the State Communication Agency (Nas.kg), and the main portal of the government (Gov.kg) were defaced at different times. However, these attacks were attributed to the overall weak security of the sites, rather than to attacks by the opposition, and all attacks were made automatically by finding vulnerability in the website. On August 24, 2014, the government portal was hacked again. According to researchers, the server had been infected with Chinese malware in 2013 that was still active at the time of the attack.

---

Lebanon

### Key Developments: June 2014 – May 2015

- Dozens of websites remained blocked over the past year, mainly for content related to escort services, Israel, gambling, or alleged child pornography (see Blocking and Filtering).

- The Ministry of Telecommunications increased internet bandwidth and decreased prices for Lebanese users, although internet speeds remain low compared to neighboring countries (see Availability and Ease of Access).

- The Cybercrimes Bureau continued to harass activists and journalists for their social media activity. In one case, security forces misled Karim Hawwa into entering the bureau and subsequently detained him for four days for sharing a political article (see Prosecutions and Detentions for Online Activities).

- Several news agencies and government municipalities had their websites hacked, with assailants threatening to delete historical archives (see Technical Attacks).
Introduction

Conditions for internet freedom in Lebanon remained somewhat static over the past year, with minor improvements in infrastructure and a decrease in violence against internet users. Disagreements among Lebanon’s political and sectarian groups about the handling of the Syrian crisis have led to an increase in hate speech on social media. Overall, the country witnessed a significant drop in violence compared to last year, although political uncertainty and economic stagnation continued. A new Council of Ministers was formed in February 2014 after 10 months without a government, and the end of Michel Sleiman’s presidential term in May resulted in another protracted power vacuum. That November, parliament voted to extend its own term until 2017, justifying the move on security concerns related to the conflict in neighboring Syria. The decision marks the second time parliament has delayed new elections, which were originally due in June 2013. Nongovernmental organizations led protests against the decision in front of the parliament building in Beirut.

Lebanese activists continued to effectively employ social media for advancing causes on digital rights, as well as for dealing with political, social, and humanitarian issues related to the plight of Syrian refugees. However, activists and journalists face potential arrest, interrogation, and threats of bodily harm for online posts critical of public officials or the army. The Bureau of Cybercrime and Intellectual Property Rights (Cybercrime Bureau), in particular, remains highly active in targeting activists, often in a manner that demonstrates little respect for the rule of law. In November 2014, Karim Hawwa reported to the bureau after he had been told he purchased a stolen smartphone, but he was instead detained for four days for sharing of a news article on his Facebook page that accused the interior minister of wrongdoing.

Lebanese citizens have historically boasted a strong tradition of freedom of the press and media pluralism. With respect to information and communication technologies (ICTs), however, the country has struggled to keep up with its more technologically advanced neighbors in the Arab world. A lack of competition in the ICT market has plagued innovation and development, although improvements to bandwidth and lower prices were seen over the coverage period. While online censorship is rare, websites owners, particularly news sites, often receive requests from courts to remove content that may be seen as defamatory. In total, 50 websites were blocked over the coverage period, mainly for content related to escort services, Israel, gambling, or alleged child pornography. Surveillance remains a strong concern in the country, particularly given the impunity of the security forces.

Obstacles to Access

Lebanon continues to struggle with poor telecommunications infrastructure, slow speeds, an urban-rural divide, and a lack of competition in the ICT sector. The state company Ogero maintains a monopoly over internet services in the country, while two state-owned mobile phone companies essentially split the mobile market between themselves. The country’s ICT development has been consistently stalled by mismanagement and political tensions, although there were some signs of improvement over the past year.

---

Availability and Ease of Access

According to the International Telecommunication Union (ITU), internet penetration in Lebanon was recorded at 75 percent at the end of 2014, up from 30 percent five years earlier. Lebanon ranked 6th in the Arab world and 62nd globally in the ITU’s ICT Development Index (IDI). However, internet speeds are relatively slow in the country. One of the main reasons for slow internet is Lebanon’s old infrastructure. Although the country commissioned a new fiber-optic network in 2011 at a cost of $55 million, reports indicate the network may not yet be in use, apparently due to a lack of bureaucratic approvals by the new administration under Telecommunications Minister Boutros Harb. The ministry stated that contractors made several errors in laying down the 4,000 kilometers of fiber-optic cables, which it has set out to fix.

Prices for internet access are set by the government. A decree by the Ministry of Telecommunications lowered fees on broadband by 44 to 68 percent as of July 2014, depending on bandwidth rates. That same month, mobile phone providers expanded the capacity of broadband bundles between 55 percent and 300 percent without changing the initial prices. Therefore, the 500 megabyte bundle was offered for a fixed price of $10, excluding TVA for both fixed and prepaid mobile users. ISPs cannot lower prices unless a decree is issued by the Ministry of Telecommunications. Tariff decree number 6297, adopted on November 9, 2011, allowed for 20 percent discounts on DSL prices in educational institutions, and decree number 8058, issued on April 25, 2012, made internet free between midnight and 7 a.m. and all day in public parks.

The Ministry of Telecommunications reported that 400 new 3G antennas were installed in December 2013, and an additional 900 antennas, more frequency, and a third channel are in progress as part of a plan to increase 3G coverage. Despite the ministry’s slow response to much-needed repairs and upgrades outside of major urban areas, some progress has been achieved in the past year. For instance, in an attempt to curb the internet penetration disparity between urban and rural areas, a recent initiative called “the Dari bundle” allows some 200,000 citizens living in 210 remote towns with no access to DSL to get free phone sets and monthly mobile internet pricing equal to the fixed DSL price. Nevertheless, some 300 villages in the rural regions of Keserwan, Batroun, Nabatiyeh, and Bekaa still lacked access, mainly due to a lack of a fixed telephone network in the area. Many in Lebanon, particularly in rural areas, experienced constant cuts to telecommunications services due to harsh weather conditions and energy cuts.

---

11 Caretaker Telecoms Minister Nicolas Sehnaoui, Facebook page, January 20, 2014, http://on.fb.me/1bEu47U.
12 Caretaker Telecoms Minister Nicolas Sehnaoui, Facebook page, January 20, 2014, http://on.fb.me/1bEu47U.
13 «رخآ راعشإ ىتح تنرتنإلا نم ةمورحم ةينانبللا قطانملا هذه [These Lebanese Regions have no access to internet till Further Notice], Annahar, April, 9, 2015, http://bit.ly/1UC5O1o.»
Lebanon

Restrictions on Connectivity

The Lebanese government maintains a monopoly over the internet backbone, as well as over the fixed and mobile telephone industry in general, allowing it to exercise tight control over internet service providers (ISPs). Lebanon has three international border gateways—in Beirut, Jdeideh, and Tripoli—where three underwater fiber-optic cables connect the country via the IMEWE, Cadmos, and Berytar cables. The gateways are operated by Ogero, a state company headed by Abdulmenaim Youssef who, in an apparent conflict of interest, also occupies a position within the Ministry of Telecommunications that oversees the operations of Ogero.

ICT Market

The Lebanese telecommunications industry is government-owned and tightly regulated. In addition to running the backbone, Ogero sets internet prices and shares in the management of online subscriptions, together with two dozen private ISPs. Lebanon has two government-owned mobile phone companies, Alfa and Touch, which are run by the private companies Orascom Telecom Holdings and Zain, respectively. Because the government sets prices and issues permits for the number of subscriptions allowed, there is little competition in the industry, and the two companies split the market evenly between themselves. The fixed-line telephone and internet network is owned and operated by Ogero, from whom all companies must purchase services.

Since no law regulates their licensing, private ISPs currently obtain a permit by decree from the Ministry of Telecommunications. Crucially, political influence can significantly interfere with the allocation of contracts to private ISPs and mobile phone operators.

Regulatory Bodies

Lebanese media and telecommunications laws are regulated by three semi-independent advisory bodies that report to the Council of Ministers. The National Council for Audiovisual Media and the Committee for Establishing Model Bylaws and Practices deal mainly with audiovisual media (TV, radio, and satellite), while the Telecommunications Regulatory Authority (TRA) is responsible for liberalizing, regulating, and developing the telecommunications sector. Overall, the three bodies remain largely powerless and fail to live up to their expectations as independent regulators in a modern state. While in theory the TRA is independent from the government, in reality, dominant Lebanese political groups possess a great deal of influence over the institution, often rendering it powerless. For this reason, the Ministry of Telecommunications remains the strongest player in the ICT domain. In fact, the past three telecommunications ministers have gone so far as to claim that the TRA has

---

18 According to the Telecommunications Regulatory Authority (TRA), it is TRA’s prerogative to assess and grant license to ISPs, but the past three ministers of telecommunication have considered that the TRA has no legal authority to do so, and the ministry has used an old law as a basis for their right to grant such license. See below for conflicts between the TRA and the Telecommunications Ministry.
Lebanon

no real authority, given that the law establishing its powers has not yet been implemented.\textsuperscript{21} Tellingly, since its launch in 2007, many of the TRA’s objectives have not been met, namely the transition from analog to digital networks and the privatization of the telecommunications sector. Yasser Fneish, senior interconnection expert at TRA, noted that the committee is finalizing a request for proposals (RFP) to purchase the adequate equipment for the digital broadcasting network.\textsuperscript{22} Similarly, the Lebanese National Committee for Transition to Digital TV has announced its work plan and launched operations to complete the transition by June 17, 2015. However, many of these issues will likely be held up by political disputes and more pressing security issues.

Limits on Content

Lebanon does not engage in significant filtering of internet content. Some 50 websites were blocked over the coverage period, mainly for content related to escort services, Israel, gambling, and alleged child pornography. Websites owners, particularly news sites, often receive requests from courts to remove content that may be seen as defamatory. Despite these limitations, Lebanon retains one of the most diverse digital landscapes in the Arab world, and several nongovernmental organizations engage in digital activism on political and social issues.

Blocking and Filtering

From 2013-14 to 2014-15, the number of websites blocked by the Lebanese government dropped from 64 to 50.\textsuperscript{23} Among the remaining websites blocked were:

- 23 websites related to escort services, blocked in accordance with articles 523 and 524 of the penal code;
- 11 Israeli sites, blocked in accordance with decree number 12562 issued April, 19, 1963 which called for the boycotting of Israel;
- 8 gambling websites, blocked according to Law 417 of 1995, which gives the “Casino Du Liban” exclusive rights to investing in gambling;
- 5 pornographic websites which allegedly promoted child pornography;
- 2 websites for breaching copyright, following a request from the U.S. government;
- 1 website, identified as being a forum for Lesbians in the Arab region, was blocked. Article 534 of the penal code criminalizes “sexual intercourse contrary to the order of nature” with up to one year in prison and has been used to prosecute LGBT individuals.\textsuperscript{24}

While many of these blocking orders have legal rooting, the order to block six pornographic websites for alleged child pornography drew the ire of some digital rights activists in the way that they

\textsuperscript{22} Yasser Fnesih, senior interconnection expert at the Telecommunications Regulatory Authority, February 7,2014, Beirut, email interview.
Lebanon

were chosen.25 The order to block the sites came after an alleged child molester in Lebanon was reported to the Bureau of Cybercrimes from a police station in Manchester, UK, which stated that the owner of the IP address in Lebanon was molesting a child in Manchester by sending her pictures of a sexual nature. Sources from the Bureau of Cybercrimes who were present during the interrogation of the accused individual revealed that the websites were chosen to be blocked because they appeared in the browser history of his personal laptop, rather than due to their publication of child pornography.26 A prominent Lebanese blogger and social media expert wrote that the websites were among the most famous pornographic websites worldwide and were unlikely to feature child pornography, given that they are not censored in other countries that ban child pornography.27

In order to block a website in Lebanon, a court order must be issued. Commonly, the court receives a complaint and files it with the Cybercrimes Bureau for further investigation, later issuing a final order to the Ministry of Telecommunications which blocks the websites through Ogero. Website owners are not notified that their websites are being blocked and must appeal the blocking within 48 hours in order to have it overturned.

YouTube, Facebook, Twitter and international blog-hosting services such as Wordpress and Blogger are freely available. In fact, Facebook, Google, YouTube, Microsoft’s Live.com, Twitter, and Wikipedia rank among the top 10 most visited websites in Lebanon.28 While most social media and communication apps are available in Lebanon, certain Voice over Internet Protocol (VoIP) applications are blocked on an inconsistent basis with the 2002 Telecom Act.29 VoIP services are mainly blocked because they cut into government revenues generated by international phone calls. In 2010, the government-owned phone company Ogero installed equipment to block VoIP throughout the network, but subsequently backed down under pressure from businesses, civil society, and politicians. Furthermore, only certain VoIP services are blocked, such as Vonage, while Skype is freely accessible.30 No clear government decision on the matter exists and the law banning VoIP remains in place, though its implementation remains vague and inconsistent. Recently, the telecoms ministry noted that it plans to allow private operators to sell VoIP services if they agree to share revenues with the state.31

While speaking at the Arab Internet Governance Forum in November 2014, Suzan Hajj Hobeiche, the head of the Cybercrimes Bureau, stated that the bureau was monitoring terrorist content in light of the rise of the Islamic State, and possessed the ability to filter such content.32 Digital media specialists in Lebanon have expressed doubt over the bureau’s abilities in this regard, though the government’s intention to filter the web is cause for concern.

26 Eyes, «لافطألاب شرحتلا ةحفاكم راطإ يف ةيحابإ عقاو ةتس بجحب رمأت ةماعلا ةباينلا» [General Prosecutor Orders the blocking of Six Porn sites].
27 Imad Bazzi, «؟نانبل يف ةيحابإلا عقاوملا تبجح اذاملو فيك» [How and Why Six Porn Websites were Banned in Lebanon], September, 3, 2014, http://trella.org/4234.
Content Removal

While filtering remains rare, there have been limited incidents in which government security officials pressured individuals and ISPs to remove certain comments—mainly criticism of government officials or the army—from social media pages, blogs, or websites. One of the most prominent instances over the past year took place in November 2014, when Judge Nadim Zwein issued a decree obliging the newspaper Al-Akhbar to remove a report from its website discussing corruption at the American University of Beirut (AUB) in response to a request from the university.33

Meanwhile, online media outlets and blogs usually have a disclaimer on their comment section making clear that they may remove any comments that include foul language or fall outside of the ethical codes. According to one expert, there is no law that clarifies who can be held liable for user generated content, such as comments. Nonetheless, there have no recent cases of intermediaries being prosecuted. 34

Media, Diversity, and Content Manipulation

Despite evidence of some filtering, taboo subjects that would normally be banned from mainstream media outlets, such as pornography, content supportive of Israel, and sectarian hate speech, are generally available online. However, self-censorship is prominent in the blogosphere and in the country’s top media outlets, which are owned by powerful figures from all sides of the political spectrum. Users often fear repercussions from the government or certain political and sectarian groups. LGBTI forums are usually banned in Lebanon in accordance with the penal code, which considers any act of advertising or supporting LGBTI issues as a crime.

Online advertising in Lebanon has grown in recent years but remains relatively weak, partly due to the slowness and unreliability of the internet. In addition, advertising agencies have yet to grasp the internet as an advertising platform, and local websites remain ill-equipped to handle sophisticated online ads.35 Whereas affluent politicians are known to purchase bulk subscriptions to newspapers and magazines in order to influence coverage, online advertising remains too small of a sector to be targeted by political groups and businesses. In fact, the majority of advertising revenue continues to go to television and other traditional media, while online sources make up two percent of the total advertising market.36

Lebanese users have access to a wide variety of local and international information sources. Reflecting Lebanon’s pluralistic society, Lebanese media is highly partisan and controlled by the dominant political-sectarian actors, mainly through direct ownership of prominent media outlets.37 For example, former prime minister Saad Hariri owns Future TV, al-Mustaqbal, the Daily Star, and a host of other online and offline media outlets. Similarly, Speaker of Parliament Nabih Berri owns National Broadcasting Network and its affiliates, while Hezbollah controls a vast network of media outlets, in-

34 Interview with President of ICT committee in the Beirut BAR association and Dr. Charbel Kareh, Head of communication committee in Internet Society - Lebanon chapter, April, 8, 2015.
Lebanon

Including al-Manar TV and al-Nour radio. The heads of these media outlets are chosen by these dominant political figures, and their news content clearly advances a particular partisan message. While ensuring plurality, this also creates a climate in which the public sphere is dominated by the agendas of powerful political-sectarian leaders and their allies, suffocating the voices of those who fall outside the main groups. At the same time, politicians are known to bribe the few independent news outlets and journalists that do exist, particularly during election periods.

Digital Activism

Civil society groups have used social media widely and effectively to mobilize support for their causes related to LGBTI rights, women’s rights, press freedom, and prisoners’ rights. Over the past year, activists used social media to lobby in support of the right to civil marriage, including the right to register children in civil marriages. Activists also revealed contradictions in Minister of Interior Nuhad el Mashnouk’s statements in support of civil marriage before he became a minister. Social media further helped activists mobilize demonstrations against the second extension of parliament’s term.

Violations of User Rights

Lebanon's weak legal environment, overzealous interrogations by the Cybercrime Bureau, and ongoing surveillance remained a grave threat to user rights over the past year. The country continues to lack a legal framework for online media, instead applying harsh defamation laws have been used to curtail investigative reporting and criticism of public authorities. While no users were reportedly sentenced to jail time over the coverage period, the Cybercrime Bureau continued to interrogate and detain individuals for their online speech, largely as an intimidation tactic. The pervasive power of the security forces is also apparent in the realm of surveillance, where blanket requests for user data have resulted in high profile political disputes between rival factions.

Legal Environment

The Lebanese constitution guarantees freedom of expression as well as freedom of the press, although those rights have not always been respected in practice. Violations of press freedom typically receive an immediate and passionate reaction from the public, serving as a powerful check against the government’s actions in this domain. However, no specific legal provisions relate specifically to online speech, and many have been anticipating a new law for over a decade. Meanwhile, courts apply these and other traditional media laws to the online sphere in an inconsistent and often contradictory fashion. This has produced a confusing legal environment with overlapping jurisdictions and contradictory laws governing online content, including the civil laws, penal code, publications law, audiovisual law, elections law, and military code of justice. Three serious attempts to develop

41 “Lebanon Parliament Extends Term,” NOW.
42 Melki, et. al., Mapping Digital Media: Lebanon, 86.
43 Melki, et. al., Mapping Digital Media: Lebanon, 89.
new media laws have generated heated national debates in the past three years, although none so far have led to any concrete results.\textsuperscript{44}

From a legal perspective, the most serious threat to internet users and online journalists remains the country's slander and libel laws. Under Article 588 of the Lebanese penal code, defaming the president carries a sentence of 3 to 12 months in prison, while defaming the army or other public figures carries a sentence of up to 6 months.\textsuperscript{45} The appeals process is often drawn out and highly politicized. In practice, however, most online users targeted with such accusations are quickly released, and the cases are usually forgotten or dropped under public or political pressure. However, even if the cases tend to wither away with little or no legal action, they almost always generate heated public debates and protests.

**Prosecutions and Detentions for Online Activities**

Court trials and prison sentences against individuals for online posts were not common over the coverage period. Instead, security forces often detain users or call them in for interrogations, particularly at the Bureau for Cybercrimes. The bureau was created in 2006 without a formal legislative decree setting out its activities or defining a "cybercrime."\textsuperscript{46} In fact, the bureau often acts with little regard to the law. In November 2014, agents misled Karim Hawwa into reporting to the bureau on the false claim that he had purchased a stolen smartphone. Instead, Hawwa was detained for four days and interrogated regarding the sharing of a news article on his Facebook page accusing Minister of Interior Nuhad al-Mashnouk of providing a contract to a company affiliated with Israel.\textsuperscript{47} Hawwa was unable to call a lawyer during the time he was held in custody, and his mother was obliged to bring in his personal laptop to the bureau, which authorities did not immediately return to Hawwa upon his release.\textsuperscript{48}

**Surveillance, Privacy, and Anonymity**

The laws regulating surveillance and the acquisition of communications data are vague and widely disputed. Attempts to develop clear privacy laws and regulations have failed, mainly because of their highly politicized nature. Currently, the typical process for acquiring user data involves a request from the Internal Security Forces (ISF) to the Ministry of Interior (or from the army to the Ministry of Defense), which is then sent to the prime minister for approval. The order is then sent to the telecommunications minister for execution—although in some instances the latter has refused to hand over the data to the ISF. This process was approved by the cabinet of ministries in 2009 as part of an agreement to share communications data with security and military officials. However, those who dispute this process, particularly the last three telecommunications ministers, cite the need to obey privacy laws, and insist that the government’s 2009 decision is limited to metadata and does not cover requests for the content of communications and other specific data. During their respective


\textsuperscript{45} Lebanese Army, “Slander and libel and sanctions in Lebanese law crimes,” [in Arabic], 2010, \url{http://bit.ly/1IYP0Wp}.


\textsuperscript{47} “Cybercrime Bureau’s ever-growing powers threatening freedoms in Lebanon,” Al Akhbar, November 22, 2014, \url{http://english.al-akhbar.com/node/22605}.

\textsuperscript{48} Samir Kassir Eyes, “[Bureau of Cybercrimes Tricks Activist Karim Hawwa and arrests him for Four Days], Skeyes Center for Media and Cultural Freedom, November, 18, 2014, \url{http://bit.ly/1JWe5Fs}.
periods in office, the ministers argued that large-scale, broad requests from the ISF should be accompanied by a court order.

Lebanon’s first draft law on personal data protection is reportedly under discussion at the parliament. While ISPs and mobile phone providers are state-owned, observers noted that data was only shared with security forces if they received a court order for a limited time interval and a limited number of users. Individuals are not usually required to show any form of ID for obtaining a prepaid SIM card, however some points of sale required it for security reasons.

**Intimidation and Violence**

Physical acts of violence in retaliation for online speech were rare in Lebanon. One incident was reported in January 2015 involving Faisal el-Qassem, an Al Jazeera journalist based in Beirut and known for his opposition to the Assad regime, who was subjected to a massive online and offline attack campaign after he shared a picture mocking the achievements of the Lebanese Army on his personal Facebook page. The campaign resulted in angry protestors breaking into Al Jazeera’s offices in Beirut demanding an apology from the Syrian journalist and filing a law suit filed against him.

**Technical Attacks**

As of 2015, the government has not yet published a strategy to defend against cyberattacks, which have been on the rise. Several government and news websites were attacked over the past year. The website of the Lebanese Patriarchy was hacked by unknown assailants in April 2014, who posted verses from the Quran. The website of the municipality of Zahleh was hacked on June 23, 2014, while Tripoli’s website was completely erased on June, 11, 2014.

The National News Agency website was brought offline for a full day on January, 13, 2015, during which it had to suspend news operations. The news website Lebanon Debate was subject to a double hacking attempt from IP addresses in Lebanon and the United States on March, 24, 2015; however, the website was able to retrieve its archive and republished under a new domain.
most well-known Lebanese and Arab blogs, Trella, was subject to a cyberattack on April 11, 2015, in which hackers threatened to erase the blog’s archive since 2004.58

Libya

Key Developments: June 2014 – May 2015

- Amid political chaos and heightened insecurity, prices for internet connections and SIM cards have increased dramatically (see Availability and Ease of Access).

- Telecommunications services have been regularly disrupted, particularly in the eastern region of the country, since the beginning of fighting between rival militias. Benghazi was cut off from all telecommunications networks for almost two months (see Restrictions on Connectivity).

- Marking one of the first instances of political censorship since the revolution, news website al-Wasat was blocked in February as a result of its frequent anti-government views (see Blocking and Filtering).

- The country’s polarized political scene has created an atmosphere of verbal harassment and threats, resulting in self-censorship, particularly among social media users (see Media, Diversity, and Content Manipulation).

- Rule of law has eroded over the past year, resulting in an absence of legal protections for online users and widespread impunity for militias and vigilante groups (see Legal Environment).

- Threats and attacks on activists and journalists increased, with some brutally murdered or kidnapped and others forced to flee Libya. At least six bloggers and activists were assassinated during the coverage period (see Intimidation and Violence).
Introduction

The situation in Libya was tenuous over the coverage period, with an ongoing political crisis and fighting between armed militias. A constitutional crisis has been in the making since November 2013, when the General National Congress (GNC), elected in July 2012, unilaterally extended its term until December 2014.\(^1\) Elections were held in February 2014 for a Constitutional Assembly to draft a new constitution, and again in June 2014 to select candidates for Libya’s House of Representatives (HOR), which was set to replace the outgoing GNC.\(^2\) However, after the elections, an Islamist-dominated faction of parliamentarians from the GNC boycotted the new HOR and instead launched a challenge with the Supreme Court for the HOR’s dissolution. Violence had been steadily increasing in the country after retired general Khalifa Haftar, who later aligned with the HOR, announced an armed campaign known as an “Operation Dignity” to rid the country of Islamist militias. Militias in Tripoli, tied to the GNC, reacted by launching their own offensive operation entitled “Libya Dawn,” which resulted in the destruction of vital infrastructure in Tripoli. A constitutional crisis ensued, in which the internationally recognized HOR met in Tobruk—due to continued fighting in Benghazi, its regular seat—and the GNC continued its activities in Tripoli, where most state institutions are located. The Libyan Supreme Court, based in Tripoli, deemed the HOR illegitimate in November 2014. Since then, the two sides have been in talks sponsored by the United Nations to formulate a national unity government.\(^3\)

The national crisis has had a devastating effect on internet freedom in the country. Prices for internet connections and SIM cards have soared due to limited availability and difficulties transporting goods within the country. Telecommunications services have been regularly disrupted due to attacks on power stations and the destruction of infrastructure; the telecommunications network was cut in Benghazi for almost two months and the telecom provider Almadar’s mobile network has been offline in the eastern part of Libya since October 2014. Marking the most significant instance of online censorship since the revolution, the news site al-Wasat was blocked in February 2014 in response to its articles against the GNC and GNC-affiliated militias. The overall lack of rule of law has contributed to an environment in which militias have violated basic human rights with impunity. At least six bloggers and activists—Tawfik Ben Saud, Sami Elkawafi, Mohamed Bettou, Mohamed el Messmari, Siraj Ghatess, and Intisar al-Hasiri were murdered during the coverage period, mainly by Islamist militias and extremists. The polarized, fraught environment has led many activists and social media users to self-censor.

Historically, access to the internet was limited to the elite. Thousands of cybercafes sprang up after 2000, however, eventually offering cheap internet to both urban and rural users.\(^4\) Over the following decade, the state telecom operator reduced prices, invested in a fiber-optic network backbone, and expanded ADSL, WiMax, and other wireless technologies throughout the country.\(^5\) In its initial stages, there were few instances of online censorship in Libya.\(^6\) However, it was not long until the regime of

---

Muammar Qadhafi began to target opposition news websites, particularly after the lifting of United Nations sanctions in 2003 led to increased access to surveillance and filtering equipment.\(^7\) Since the overthrow and death of Qadhafi in 2011, the country has witnessed a flurry of self-expression, resulting in an increase in news sites and massive growth in Facebook use.\(^8\) However, the 2011 civil war and subsequent fighting has taken a heavy toll on the country’s information and communications technology (ICT) sector, damaging infrastructure and sideling an earlier US$10 billion development plan that had been set to be complete by 2020.\(^9\) Laws that once prohibited criticism of the revolution that brought Qadhafi to power have been changed to outlaw criticism of the 2011 revolution that removed him. In short, significant obstacles to access remain in the country and numerous violations against user rights were witnessed over the coverage period.

### Obstacles to Access

*Internet access has been badly affected by the ongoing conflict. Electricity outages and physical damage to infrastructure have limited connectivity. Despite that, there has been an increase in the number of internet users, particularly among youth. Quality of service remains poor and the ICT sector remains monopolized by state-owned entities.*

### Availability and Ease of Access

Internet penetration has traditionally been very low in Libya. According to figures from the International Telecommunication Union, internet penetration was at 17.8 percent at the end of 2014, up from 10.8 percent five years earlier.\(^10\) Some 350 telecommunications towers in 19 different locations provide WiMax and other internet services. WiMax subscribers make up the majority of total subscriptions in the country according to the latest data published by the government, with some 448,135 subscribers compared to 149,963 subscribers for ADSL and 76,885 for LibyaPhone.\(^11\) Broadband was introduced in 2007, although the number of fixed broadband subscriptions was relatively low at just over 1 subscription per every 100 inhabitants in 2013, the last year in which data was available.\(^12\) Since July 2014, WiMax service has been unstable in many parts of the country, especially in Benghazi and other cities in the east, due to the destruction of WiMax towers during fighting.\(^13\)

Mobile phone use is ubiquitous, with over 10 million mobile subscriptions in Libya, representing a penetration rate of 161 percent.\(^14\) Prices have dropped precipitously since the introduction of a second mobile provider in 2003, resulting in greater affordability and opening the market to competition, although both operators are owned by the state-owned Libyan Post Telecommunications and Information Technology Company (LPTIC). By 2013, the price of a prepaid SIM card from the main provider, Libyana, was LYD 5 (US$ 4), compared to LYD 1,200 (US$889) in 2003. Smartphones and

---

11. Data about internet users in Libya on LPTIC Facebook page, accessed May 10, 2015, [http://on.fb.me/1LnX6MM](http://on.fb.me/1LnX6MM).
Libya

3G connectivity have been available since 2006, though the prohibitive cost of compatible handsets impedes their wider dissemination.\textsuperscript{15} The service from Almadar, another mobile company, has been unreliable in the eastern part of the country since the 2011 revolution, and since October 2014, has been permanently down. In turn, prices for a Libyana SIM rose to LYD 25 (US$ 18) due to vandal attacks on Libyana offices throughout the country and a limited number of Libyana offices in Benghazi, resulting in limited access to SIM cards in the city.

Similarly, the cost of a home internet connection remains beyond the reach of a large proportion of Libyans, particularly those living outside major urban areas. A dial-up internet subscription cost LYD 10 (US$8) per month, an ADSL subscription was LYD 20 (US$ 16) for a 20 GB data plan, and WiMax service was LYD 40 (US$ 31) for a 15 GB data plan, after initial connection fees. By comparison, gross national income per capita was US$ 1,078 per month, pushed up by relatively high salaries in oil and gas firms.\textsuperscript{16} Libya Telecom and Technology (LTT) has decreased WiMax connection fees for individual users from LYD 160 (US$ 124) to LYD 120 (US$ 93) and from LYD 260 (US$ 202) to LYD 220 (US$ 171) for households.\textsuperscript{17} WiMax modems are in short supply, resulting in high prices for second-hand devices sold on the site Open Souk, Libya’s online marketplace.\textsuperscript{18}

Many foreign and Libyan organizations and individuals in need of reliable internet service have been driven towards two-way satellite internet technology. As two-way technology has become more popular, connection fees and equipment costs have lowered. Prices were recently at LYD 800 (US$ 630) for the hardware, while a monthly subscription costs LYD 255 (US$ 210) for a fast connection, depending on the number of users.\textsuperscript{19}

Most people access the internet from computers in their homes and workplaces, with mobile phones being the next most common point of access. The cybercafe industry was decimated in many parts of Libya; instead, cafes and restaurants partner with local internet businesses to offer Wi-Fi hotspots with different data plans. The adult literacy rate was last recorded at 90 percent and a wide range of websites and computer software is available in Arabic.\textsuperscript{20} However, limited computer literacy, particularly among women, has been an obstacle to universal access.

The Libyan civil war significantly disrupted the country’s telecommunications sector, with the damage estimated at over $1 billion.\textsuperscript{21} There have been few improvements to ICT equipment since the Qadhafi era, prompting frustrated Libyans to create the Facebook page titled, “I hate Libyan Telecom and Technology,” which attracted over 23,000 followers.\textsuperscript{22} Upgrades have been proposed in an effort to respond to demands for increased capacity, such as the laying of the European Indian Gateway and Silphium submarine cables,\textsuperscript{23} the construction of additional WiMax towers,\textsuperscript{24} the creation of

\textsuperscript{21} Lancaster, Libya – Telecoms, Mobile and Broadband.
\textsuperscript{22} See I hate Libya Telecom and Technology (LTT), Facebook Business Page, https://www.facebook.com/ihateltt.
Wi-Fi hotspots, the installation of a long distance fiber-optic cable within the country, and the development of next-generation broadband. Although there have been many announcements of partnerships between Libyan telecommunication companies and foreign companies, such as Alcatel Lucent and Samsung, the status of these contracts are unknown, reflecting the lack of transparency in the Libyan ICT sector.

According to Akamai, Libya has the world’s slowest internet speeds at 0.5 Mbps. ICT experts say this is due to poor infrastructure, a lack of quality of service (QoS), technology constraints, and a continued lack of regulations. Furthermore, broadband is not widely available, bandwidth limitations exist for fixed-line connections, wireless users face slower speeds due to heavy congestion during peak hours, and there is a general lack of resources and personnel to perform maintenance and repairs.

Restrictions on Connectivity

Since February 2011, Libya has seen repeated shutdowns to internet service due to vandalism and technical disruptions. Violent clashes in Benghazi caused the telecommunications network in the area to stop working for almost two months during the coverage period. The Almadar mobile network has not been working in the eastern part of Libya since October 2014. Although phone services have been restored in some areas, power and telecommunication services remain unstable with frequent cuts. Internet users in Tripoli also noticed slow speeds on Wimax and ADSL services in April 2015, a month which also saw disruptions in access. Some users stated on Twitter that the LTT had deliberately cut off access to restrict the spread of information surrounding events in Tripoli, while the LTT stated that the blackout was due to an organized attack. WiMax service was cut for two months in the city of Sirte because of fighting. The LTT has not compensated those affected by the long service disruptions, creating a sense of dissatisfaction among LTT users in the affected cities.

36 “LTT claims internet was halted due to attack by 13 international pirates,” Libya Herald, April 28, 2015, http://bit.ly/1P7aNY.
ICT Market

The state-run Libyan Post Telecommunications and Information Technology Company (LIPTC), formerly the General Post and Telecommunications Company (GPTC), is the main telecommunications operator and is fully owned by the government. In 1999, the GPTC awarded the first internet service provider (ISP) license to Libya Telecom and Technology (LTT), a subsidiary of the state-owned firm. Since the fall of the regime, 25 ISPs have been licensed to compete with state-owned ISPs and 23 VSAT operators have also been established. Many are based in Tripoli and have strong ownership ties to the government. LIPTC owns two mobile phone providers, Almadar and Libyana, while a third provider, Libya Phone, is owned by LTT.

There has been a noticeable increase in the number of companies and agencies working to provide alternative methods to connect to the internet, such as through satellites (VSAT). On the other hand, there have been few developments within the mobile market. Although there were plans to put Almadar on the stock exchange and to issue the country’s first tender for a private mobile license, the country has yet to witness any significant liberalization in the sector.

Regulatory Bodies

The post-conflict regulatory environment remains very unclear. There are disputes over the country’s governance, which have led to conflicts. During the Qadhafi era, decisions on licensing were made by the government-controlled GPTC (now LPTIC). After the revolution, the transitional government established the Ministry of Communications and Informatics to oversee the country’s telecommunications sector. The ministry runs the sector through two main bodies: the General Authority of Telecommunications and Informatics (GATI), formerly the General Telecom Authority, and Libyan Post Telecommunications and Information Technology Company (LPTIC), formerly GPTC. GATI is responsible for policymaking and regulations, whereas LPTIC is a holding company for all telecommunications service providers in the country. Libya’s top-level domain, “.ly,” falls under the responsibility of LTT. Registrations are handled by Register.ly on behalf of NIC.ly.

In 2014, the Ministry of Communications and Informatics appointed a committee to draft a new Telecommunication Act, to set standards for the sector and replace the existing legislation surrounding ICT regulations. The act will include also create an independent Telecommunication Regulatory Authority (TRA).

---

Libya

Limits on Content

Limits on content have been rare in Libya since the overthrow of the Qadhafi regime in 2011. The lifting of restrictions has resulted in a diverse online media landscape and an improved market for online advertising. Facebook, in particular, has become an important news source for many Libyans; many government bodies post official statements directly to the social network. Nonetheless, the quality of the content published on these platforms remains poor and highly polarized. Decades of oppressive rule and the continued threat posed by militias has contributed to some degree of self-censorship among users, particularly on sensitive subjects.

Blocking and Filtering

After several years of openness, the first instance of politically motivated blocking since the Qadhafi era was seen this year with the blocking of Alwasat.45 The news site, which has published views against the GNC and Libya Dawn, was blocked on February 10, 2015 by the LTT, apparently due to a legal order from a court in Tripoli. An announcement revealing the blocking order was not made until April, when the LTT posted a statement to its Facebook page.46 Human rights activists and social media users protested the decision using the hashtag “#No2FajrCensorship” on the occasion of World Press Freedom Day on May 3, 2015.

YouTube, Facebook, Twitter and international blog-hosting services are freely available. Some pornographic websites have been blocked since the end of the civil war based on a decision made by an ad hoc Temporary Steering Committee formed after the fall of Qadhafi and the liberation of Tripoli.47 Prior to the war, “indecency” was prohibited but sexually explicit sites were never blocked. The LTT has not unblocked the content, perhaps due to the conservative outlook of some political factions vying for influence in the future of Libya. A 2006 law mandates that websites registered under the “.ly” domain must not contain content that is “obscene, scandalous, indecent or contrary to Libyan law or Islamic morality.”48

In February 2014, LTT blocked an additional set of pornographic sites and mistakenly blocked the Wordpress.com domain for a few days. It was unblocked following requests from Libyan bloggers.49 On April 18, 2015, Facebook was reportedly inaccessible for a few hours in some areas of Tripoli. LPTIC denied responsibility for the interruption, instead releasing a statement reiterating its commitment to free speech and insisting that the interruption had been caused by armed groups taking control of the LTT.50

There is little transparency and no legal framework related to the blocking of websites in Libya, as

---

regulations have yet to be formulated. Officially, all regulations from the Qadhafi era remain valid. When accessing a banned website, users are shown a message from the authorities noting that the site has been blocked. As most state institutions are based in Tripoli, the internationally recognized House of Representatives (HOR), which is based in Tobruk, does not seem to have access or control over the country’s telecommunications services.

Content Removal

Authorities do not frequently request private providers or intermediaries to delete content. Rather, there are coordinated efforts to “report” Facebook pages for deletion, particularly for political views against militias. Separately, many Qadhafi-era government webpages containing information on laws and regulations from before the uprising are inaccessible, as is the online archive of the old state-run Libyan newspapers. Some of these websites may have become defunct after the officials running them were ousted or hosting fees were left unpaid, but others were likely taken down deliberately when the revolutionaries came to power.

Media, Diversity, and Content Manipulation

After a sudden opening of the online media landscape after the fall of Qadhafi, negative trends such as self-censorship, verbal harassment, and a lack of quality reporting now characterize Libya’s online sphere. The 2011 revolution brought a notable increase in the number of bloggers writing within Libya, particularly on issues related to political activism, hope for the future, and government criticism. However, a sizable number of Libyan bloggers, online journalists, and ordinary citizens continue to practice some degree of self-censorship due to continued instability and increasing threats and violence against journalists over the past years.\(^5\) Social taboos such as sexual abuse or conflicts between warring tribes and rival cities are off-limits. Online writers also shy away from expressing religious opinions for fear of being marked as an atheist or a Shiite sympathizer, both of which can be life-threatening. Many commentators avoid criticizing the 2011 revolution, General Haftar, the GNC, and Libya Dawn, mainly out of fear of retribution from armed groups and nonstate actors.

Despite the growth in self-censorship, the online media landscape remains much more diverse than in previous years, with few dominant news providers and several privately owned outlets. Many of Libya’s online outlets have clear political agendas and lack quality journalism and professionalism, instead publishing incitement and propaganda. The low levels of reliability and credibility have made it difficult for many to find neutral and objective sources of news about Libya.\(^5\)

The online advertising market has grown slowly and websites related to the Amazigh (whose language was banned under Qadhafi) and other minorities are now flourishing.\(^5\) Interestingly, Facebook is often the platform of choice for city and even government officials to publish updates and official communication. From April 2012 to April 2013, the number of Facebook users in Libya doubled from some 400,000 to 860,000.\(^5\) The social networking site was the most visited website in the country.

Libya

and has also become the main source of news about Libya for a large number of users inside and outside the country.\textsuperscript{55} The latest available figures on Facebook use among Libyans recorded some 25.8 percent using the service in 2014.\textsuperscript{56}

Digital Activism

Over the past years, Libyans have used Facebook and Twitter to mobilize around a variety of causes. Recent campaigns include the "No Extension of GNC" movement, when social media users protested the decision of the GNC to remain in power past the transitional deadline of February 7, 2014. The move prompted massive protests in Benghazi's Freedom Square, which quickly spread into violent clashes around the country. Since 2014, Libyan activists have promoted democratic values, campaigned against incitement, and dismissed propaganda on Facebook. Most of these campaigns started and spread through hashtags, reflecting the impact of hashtag activism on creating change in Libya.

One of these campaigns was #IAmTawfik,\textsuperscript{57} launched after the death of two young activists in Benghazi. It was created to promote peace and hope in Libya's future, as well as to show the resilience of the country's youth and civil society in the face of targeted killings of those fighting for a free Libya. An online campaign in the lead up to the month of Ramadan asked landlords to decrease rental prices for displaced families in Benghazi.\textsuperscript{58} The campaign was well received and had a notable effect on the ground. Other trending campaigns included "Say yes to resuming schools in Benghazi;"\textsuperscript{59} #MyLibya,\textsuperscript{60} a social media campaign to show the bright side of Libya; #IWantMyCountryBack,\textsuperscript{61} launched on Twitter to express Libyans' anger at the current state of affairs; and "Benghazi will not kneel,"\textsuperscript{62} a collective online effort to assemble people to the streets for a massive demonstration against the Islamist extremist group Ansar Alsharia and affiliated groups in August 2014.

Violations of User Rights

Freedom of opinion, communication, and press are guaranteed by Libya’s Draft Constitutional Charter, released by the Libyan Transitional National Council in September 2011.\textsuperscript{63} However, delays in the drafting of a constitution and the general absence of law enforcement have contributed to weak rule of law in the country. The laws that do exist on the books remain, for the most part, carried over from the Qadhafi era. The gravest threats to user rights, however, came from armed groups during the coverage period. Several online journalists have faced threats and, in some cases, violent attacks due to the country's highly polarized environment.

\textsuperscript{58} Social media coverage of the decreasing the rental price campaign, May, 2015. Facebook https://goo.gl/WmKlGj; Twitter, #ضفخ_كراجيا_كناضمر_كرابم https://goo.gl/l7NLOfo
\textsuperscript{59} Facebook page of the campaign [in Arabic], https://goo.gl/znZNTL
\textsuperscript{60} "Amid chaos, Libyans took on the bright side," BBC Trending, June 11, 2014, accessed July, 9, 2015, http://bbc.in/1N2m5yE
\textsuperscript{61} "Libyans refuse to give up their country, sharing their feelings with hashtag #IWantMyCountryBack," Your Middle East, December 27, 2014, accessed July, 9, 2015, http://bit.ly/1RbDkFQ
Legal Environment

Several Qadhafi-era laws remain on the books due to the absence of any significant legal reform in the country since the revolution. Harsh punishments remain for those who publish content deemed offensive or threatening to Islam, national security, or territorial integrity. A law on collective punishment is particularly egregious, allowing the authorities to punish entire families, towns, or districts for the transgressions of one individual. Because of their vague wording, these laws can be applied to any form of speech, whether transmitted via the internet, mobile phone, or traditional media. When new laws have been passed, changes have been cosmetic. In February 2014, the GNC amended Article 195 of the penal code to outlaw any criticism of the 2011 “February 17 Revolution” or its officials, as well as members of the GNC, using similar language to that used to outlaw criticism of Qadhafi’s “Al-Fateh Revolution.” The judiciary has gained in independence since 2012, when, in a landmark decision, the Supreme Court of Libya declared a law that criminalized a variety of political speech unconstitutional. More recently, however, state bodies remain subject to pressure from a variety of armed militias.

Prosecutions and Detentions for Online Activities

Law enforcement was sparse of over the coverage period, due to the ongoing conflict. There were no reported arrests of individuals for their online activities over the coverage period, although extralegal violence by militias was prevalent (See “Intimidation and Violence”).

Surveillance, Privacy, and Anonymity

Uncertainties remain over the actions of domestic intelligence agencies in the new Libya. A July 2012 report from the Wall Street Journal indicated that surveillance tools leftover from the Qadhafi era had been restarted, seemingly in the fight against loyalists of the old regime. Others suspect that these tools were activated to target those with an anti-Islamist agenda. During an interview on al-Hurra TV in March 2012, the Minister of Telecommunications stated that such surveillance had been stopped because the interim government wanted to respect the human rights of Libyans. An organization representing IT professionals in Libya refuted his remarks in an online statement, saying telecom sector employees had confirmed that the surveillance system was reactivated. Its status in 2014 was unclear. Given the lack of an independent judiciary or procedures outlining the circumstances under which the state may conduct surveillance, there is little to prevent the government, security agencies, or militias who have access to the equipment from abusing its capabilities.

The Qadhafi regime had direct access to the country’s DNS servers and engaged in widespread surveillance of online communications. State of the art equipment from foreign firms such as the

French company Amesys, and possibly the Chinese firm ZTE, were sold to the regime, enabling intelligence agencies to intercept communications on a nationwide scale and collect massive amounts of data on both phone and internet usage. Correspondents from the Wall Street Journal who visited an internet monitoring center after the regime’s collapse reportedly found a storage room lined floor-to-ceiling with dossiers of the online activities of Libyans and foreigners with whom they communicated.

After the capture of Tripoli by armed militias, many concerns have been raised over the role of LPTIC in monitoring mobile and internet communication, particularly from individuals in Benghazi. Although LPTIC released an official statement denying the accusations on its Facebook page, its involvement in political and security affairs remains vague among many Libyans.

### Intimidation and Violence

The breakdown of the rule of law and the growing influence of militias has resulted in a worrying uptick in threats and violence against online journalists and activists. Since the end of 2011, the country has experienced a wave of killings and attacks against activists and journalists. According to Human Rights Watch, most were politically motivated. The following cases were reported during the coverage period:

- Two young activists, Tawfik Ben Saud and Sami Elkawafi, were killed on September 19, 2014. The identity of the shooter was unknown, but many linked the attacks on armed groups and extremists. Both were leading bloggers and social media activists involved in organizing demonstrations and promoting peace and democracy.

- Mohamed Bettou, Mohamed El Messmari, and Siraj Ghatess, three bloggers and activists well known for their outspoken support of human rights, were brutally killed in November 2014 in the eastern city of Derna, home to many extremists.

- In February 2015, blogger and civil rights activist Intisar al-Hasiri was found dead in her vehicle, apparently having been shot in the head. Al-Hasiri was an outspoken advocate of human rights, rule of law, and democracy in Libya.

- Moez Bannon, a political and social media activist based in Tripoli, has been reported missing since July 2014 after he spoke out against the city’s militias.
Libya

Tension and conflict has resulted in an overall increase in online hate speech, defamation, harassment, and even death threats. In late 2014, militias and extremists used Facebook to target and silence activists.79 For example, anonymous users set up a Facebook page featuring the names, photos, and addresses of Benghazi activists calling for their assassinations and kidnapping. The page was taken down after online activists reported it.80

Technical Attacks

Websites are highly vulnerable to cyberattacks in Libya, with prominent news sites such as Libya Herald employing protection measures against distributed denial-of-service (DDoS) attacks. No similar examples were reported during the coverage period. Anti-militia Facebook pages were consistently hacked or closed down after mass reporting by users, a significant concerning given that most Libyans consider Facebook to be their main source of news.

Malawi

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>Partly Free</td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>16</td>
<td>15</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>15</td>
<td>13</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>42</td>
<td>40</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 16.8 million
Internet Penetration 2014: 6 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2015 Status: Partly Free

Key Developments: June 2014 – May 2015

- In May 2015, the Malawian parliament implemented a 10 percent excise duty on mobile phone text messages and data transfers through both internet and mobile services (see Availability and Ease of Access).

- Anecdotal reports suggest that government officials regularly require editors of online news websites take down certain objectionable content (see Content Removal).

- Suspected government sponsored trolls quieted down under the new government elected in May 2014, suggesting that the strategic pattern of infiltration observed under former presidents was no longer practiced (see Media, Diversity, and Content Manipulation).

- There were no arrests or prosecutions for online activities during the coverage period, compared to Malawi’s former leadership when online journalists were periodically detained and prosecuted for critical articles posted on news websites (see Prosecutions and Detentions for Online Activities).

- The Consolidated ICT Regulatory Management System (CIRMS)—known locally as the “spy machine”—was implemented in March 2015, enabling the communications regulator to access subscriber’s data and communications without judicial oversight (see Surveillance, Privacy, and Anonymity).
**Introduction**

Access to the internet remained the greatest obstacle to internet freedom in Malawi during the coverage period, as low internet and mobile phone penetration rates lagged significantly behind most countries in the region and the world. High costs continued to hinder access to information and communication technologies (ICTs), which were partly due to hefty value-added taxes on both internet and mobile phone services that make access prohibitively expensive for a large majority of Malawians. Prices are likely to increase further under a new tax policy announced in May 2015 that levies a 10 percent excise duty on mobile phone text messages and data transfers through both internet and mobile services. The highly criticized internet tax also threatens to increase the costs of banking and mobile money services.

Arthur Peter Mutharika, the younger brother of and close advisor to the former president Bingu Wa Mutharika (who died in April 2012) was elected president in May 2014. Citizens and observers were concerned the new president would take after his late brother and unleash a repressive campaign against the media and civil society while in office, but to date, such concerns have not materialized. And in contrast to former President Joyce Banda, Mutharika has not targeted internet users or online journalists for critical commentary, though anecdotal reports suggest that government officials regularly require editors of online news websites take down certain objectionable content.

Apart from the new regressive tax on ICTs, the new government under President Mutharika has enacted a number of positive ICT development policies in its first year. The launch of the Malawi Internet Government Forum in July 2014 connected various stakeholders in the development of Malawi’s internet policies and infrastructure. The government also announced plans to set up a Universal Access Fund (UAF) to help telecommunication operators provide services to rural areas characterized as difficult and economically unviable. Nevertheless, the controversial regulatory system first introduced under the late President Mutharika in 2011, critically known as the “spy machine,” was implemented in March 2015, leading to concerns of potential government access to user data on mobile phone networks without judicial oversight.

**Obstacles to Access**

*High taxes, poor infrastructure, and the lack of a local internet exchange point, among other obstacles, make access to ICTs prohibitively expensive for the majority of Malawians, resulting in low access rates across the country. A 10 percent excise duty on mobile messaging and data transfers introduced in May 2015 will further impede access.*

**Availability and Ease of Access**

As a landlocked and densely populated country that suffers from widespread poverty, Malawi has one of the lowest rates of internet access in the world. According to the International Telecommunication Union (ITU), internet penetration stood at less than 6 percent in 2014, up slightly from 5 percent in 2013.\(^1\) Fixed broadband subscriptions are extremely rare in the country, reaching only 0.05

---

percent of the population in 2014,\textsuperscript{2} while mobile phone penetration in Malawi is also relatively low at 31 percent,\textsuperscript{3} compared to an average of 72 percent across the continent.\textsuperscript{4}

Low rates of internet and mobile phone access in Malawi are largely a result of high costs, which include expensive value-added taxes (VAT) of 17.5 percent on mobile phones and services, and a VAT of 16.5 percent on internet services, the costs of which are borne by consumers.\textsuperscript{5} In May 2015, the Malawian parliament implemented an additional 10 percent excise duty on mobile phone text messages and data transfers through both internet and mobile services.\textsuperscript{6} Local economists and critics argue that this will also lead to increases in banking and mobile money services, discouraging further uptake of these important digital services.\textsuperscript{7}

Consequently, mobile phone use is extremely expensive for average Malawians, who use over 56 percent of their average monthly earnings on mobile phone services, according to the ITU.\textsuperscript{8} By contrast, Kenyans and South Africans spend less than 5 percent of their monthly earnings.\textsuperscript{9} As of mid-2015, the monthly price of fixed-line internet access cost US$16.50, while a monthly mobile 3G data plan cost about US$24 for 1.5GB of data, prices that are beyond the reach of the majority of Malawians.

Very few households have computers with access to the internet at home, thus most users log on at cybercafes, which charge a minimum of MWK 15 per minute, or about US$2.00 per hour, and close at 6pm. However, patronage at local cybercafes has declined because of increased mobile internet access with the introduction of 3G and 3.75G mobile broadband services. DSL and WiMAX wireless broadband services are available, while competition between private ISPs has further enabled wireless internet access through Wi-Fi hotspots, particularly in urban areas. Nonetheless, broadband speeds are still slow at 1.90 Mbps (compared to a global average of 3.9 Mbps), according to May 2015 data from Akamai’s \textit{State of the Internet} report.\textsuperscript{10}

Very few households have computers with access to the internet at home, thus most users log on at cybercafes, which charge a minimum of MWK 15 per minute, or about US$2.00 per hour, and close at 6pm. However, patronage at local cybercafes has declined because of increased mobile internet access with the introduction of 3G and 3.75G mobile broadband services. DSL and WiMAX wireless broadband services are available, while competition between private ISPs has further enabled wireless internet access through Wi-Fi hotspots, particularly in urban areas. Nonetheless, broadband speeds are still slow at 1.90 Mbps (compared to a global average of 3.9 Mbps), according to May 2015 data from Akamai’s \textit{State of the Internet} report.\textsuperscript{10}

A low literacy rate of 64 percent and a significant digital gender divide also hinders access to ICTs, while unreliable electricity and the high cost of generator power in the country strain ICT use. Less than 9 percent of the country has access to electricity, giving Malawi one of the lowest electrification rates in the world, according to the World Bank.\textsuperscript{11} The electricity grid is concentrated in urban centers, but only 25 percent of urban households have access, compared to a mere 1 percent of rural households. Half of formal sector enterprises in Malawi rely on backup generators. Meanwhile, the high costs of infrastructural development in rural areas has led to an unwillingness to invest in the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{2} ITU, “Fixed (Wired) -broadband Subscriptions, 2000-2014,” \url{http://bit.ly/1FDwW9w}.
\item \textsuperscript{3} ITU, “Mobile-cellular Telephone Subscriptions, 2000-2014,” \url{http://bit.ly/1FDwW9w}.
\item \textsuperscript{6} WangaGwede, “Malawi hikes tax on internet, duty on SMS: Goodall says local resources to finance 2015/16 budget,” Nyasa Times, May 23, 2015, \url{http://bit.ly/1Mh08jG}.
\item \textsuperscript{7} “J-Lu takes a swipe at Malawi’s SMS and internet tax, labels it ‘Retrogressive and anti-democratic,’” Malawian Watchdog, May 25, 2015, \url{http://bit.ly/1GoN8es}.
\item \textsuperscript{8} Emmanuel Igunza, “Malawi’s expensive mobile phone habit,” BBC, February 20, 2015, \url{http://bbc.in/1vkTJ4E}; International Telecommunication Union, Measuring the Information Society Report 2014, \url{http://bit.ly/1FIO8ff}.
\item \textsuperscript{9} Igunza, “Malawi’s expensive mobile phone habit.”
\item \textsuperscript{10} Akamai, “Average Connection Speed,” map visualization, \textit{The State of the Internet}, 2015, accessed May 29, 2015, \url{http://akamai.me/1L55K0D}.
\item \textsuperscript{11} Latest available data is from 2010. World Bank, “Access to electricity (% of population),” accessed May 29, 2015, \url{http://bit.ly/1zN9eaf}.
\end{itemize}
\end{footnotesize}
country’s remote regions, though the regulatory authority is looking to subsidize fees to encourage operators to deploy ICT services in the country’s less profitable yet neediest areas.

To address the country’s access issues, the government launched the Malawi Internet Government Forum in July 2014 to connect various stakeholders in the development of Malawi’s Internet policies and infrastructure. Moreover, the Malawi Communications Regulatory Authority (MACRA) announced in September 2014 plans to set up a Universal Access Fund (UAF) to help telecommunication operators provide services to rural areas characterized as difficult and economically unviable.

**Restrictions on Connectivity**

The country’s ICT backbone is entirely national in nature, with no regional integration yet in place. Due to Malawi’s landlocked location, the country’s connection to the international fiber network runs through Mozambique, Zambia, South Africa, and Tanzania through the SEACOM and EASSy networks. Three new submarine cables are currently competing to be the first to start service in Malawi as the country plans to extend a fiber-optic backbone through Tanzania to the coast. If a suitable regulatory regime is also put in place, the new cables should bring down the cost of international bandwidth and boost the broadband market.

The government of Malawi does not have centralized control over the international gateway, which the ITU characterizes as fully competitive. ISPs have their own gateways through the SEACOM and EASSy networks and operate internet exchange points. The state-owned Malawi Sustainable Development Network Programme (SDNP), a fully licensed ISP, oversees the local traffic hub that connects all ISPs in the country but does not have the capacity to block content or restrict connectivity.

**ICT Market**

Although Malawi is categorized as a least developed country, it has experienced strong economic growth over the recent years, reaching nearly 6 percent in 2014. According to a government source, the ICT sector contributed nearly 4 percentage points to the country’s GDP in 2014, up from 3.5 percentage points in 2010.

There are 22 licensed ISPs in Malawi, all of which are privately owned, with the exception of the Malawi Sustainable Development Network Programme (SDNP). One ISP, Malawi Telecommunications Limited (MTL), also serves as the country’s telecommunication backbone, leasing its infrastructure to most ISPs and mobile phone service providers in the country. Previously a government-owned entity, MTL was privatized in 2005; at present, the government retains 20 percent of MTL’s shares while Telecomm Holdings Limited holds the other 80 percent.

17 Author interview with IT engineer for a local mobile phone company on March 25, 2015.
18 Gondwe, “Malawi forms Internet Governance Forum.”
Malawi

Market competition for mobile phone providers expanded with the introduction of a converged licensing regime in 2010, which enabled the country’s two fixed-line operators, MTL and Access Communications, to enter the mobile market, giving Malawi a total of four mobile phone providers.21 Airtel Malawi and Telecom Networks Malawi are the other two mobile providers and together command a mobile teledensity of 18 percent. A third mobile operator, G-Mobile, was licensed in 2008, but the rollout of the new network experienced delays. As of 2015, G-Mobile is still in court appealing the revocation of its license due to a failure to start services on time.22 A fourth license was awarded to Celcom in 2011, and although the launch of its services was expected in 2013, it asked the regulator MACRA in September 2013 to extend its rollout period for another three years.23

The high cost of internet access in Malawi is also a result of the many challenges that ISPs face, one being the lack of a local internet exchange point, which forces telecoms to rely on upstream service providers that are usually based outside of Africa. As a result, data that should be exchanged locally within Malawi or regionally must pass through Europe or North America where upstream providers are based, leading to an unnecessary and expensive waste of upstream bandwidth. Furthermore, currency devaluation amid a weak economy since 2012 has prevented telecoms from upgrading their networks.24

Regulatory Bodies

The Malawi Communications Regulatory Authority (MACRA) is the country’s sole communications regulator, established under the 2008 Communication Act to ensure reliable and affordable ICT service provision throughout Malawi. Its mandate is to regulate the entire communications sector and issue operating licenses for mobile and fixed-line phone service providers, ISPs, and cybercafes.

Political connections are often necessary to receive such licenses. Moreover, the institutional structure of MACRA is subject to political interference, with its board comprised of a chairman and six other members appointed by the president and two ex-officio members—the secretary to the Office of the President and Cabinet and the Information Ministry secretary.25 The director general of MACRA, whose appointment also passes through the president’s scrutiny, heads the authority’s management and supports the board of directors in the execution of its mandate.

Limits on Content

The common pattern of progovernment infiltration on social media and in online news outlets seemed to subside under the new president elected in May 2014, though anecdotal reports suggest that government officials regularly required editors of online news websites take down certain objectionable content.

Blocking and Filtering

---

21 Henry Lancaster, Malawi - Telecoms, Mobile and Broadband - Market Insights and Statistics, Executive Summary.
24 Henry Lancaster, Malawi - Telecoms, Mobile and Broadband - Market Insights and Statistics, Executive Summary.
The current government of Malawi does not block or filter internet content aside from pornography, which ISPs block at internet exchange points in the country. Social media platforms are freely available in Malawi. Governments under former presidential regimes, however, have censored internet content in the past.26

Content Removal

There is a strong sense that the government forces editors of online news websites to take down certain content deemed objectionable, though the extent of the practice is widely underreported in Malawi. One case anecdotally documented in 2015 involved an article on Nyasa Times that accused President Peter Mutharika’s Special Aide Ben Phiri of corruption and bribery, which disappeared from the news website within 30 minutes of publication. Observers believed the takedown was in keeping with the media’s common practice of yielding to government pressure exerted behind the scenes.

Media, Diversity, and Content Manipulation

Malawi’s online media landscape does not reflect a wide diversity of viewpoints, primarily due to the low level of internet users in the country. Economic conditions in the country have also made it difficult for journalists and media groups to launch online outlets alongside the high cost of using the .mw domain—currently administered by the Malawi SNDP on behalf of the Malawian government—make it expensive to provide locally-produced content. According to an official at the SDNP, the cost of using the .mw domain is US$100 per month for the first two months after registering for the domain, and US$50 per month thereafter. Furthermore, online advertising is low due to a limited understanding of the internet among businesses and their hesitancy to advertise with independent media outlets.

Nevertheless, the growing blogosphere is regarded as an important aspect of journalism in Malawi, with Malawian journalists frequently winning the Media Institute of Southern Africa’s annual blogging award. Media publishers such as Blantyre Newspapers Limited often host bloggers on their websites to enhance their image as independent news sources.

Online users and commentators practice a degree of self-censorship but are generally more open to discussing topics of controversial nature. In contrast, online journalists usually exhibit caution when handling news associated with ethnic, racial, or religious minorities.

There was little to no government or partisan manipulation of online content during the coverage period. Since the new government was elected in May 2014, progovernment trolls have quieted down, suggesting that the strategic pattern of progovernment infiltration on social media and online news websites to attack commentary that was critical of the government is no longer being practiced. Even the government’s news website MANA Online, which was launched in August 2012 to compete with dissenting online news outlets in the country,27 simmered down its progovernment line since the election. The Banthu Times—another propaganda online news outlet established by the Presidential Press Secretariat under President Joyce Banda to counter dissenting news online—

Malawi

no longer publishes content that is aligned with the government. The current press secretariat has not replaced the outlet, preferring instead to publish news on the State House website.

Digital Activism

The most influential ICT tool in Malawi is the mobile phone through which SMS messages are used to organize demonstrations, garner political support, and conduct opinion polls. The positive impact of mobile phones and new communication applications was particularly pronounced in the lead-up to the May 2014 tripartite elections, as candidates vying for the presidency, parliament, and local councils made extensive use of SMS and social media platforms to engage with voters. In addition, citizens were able to verify their voter registration on their mobile devices for free, encouraging high voter turnout.28

Significant social media commentary and activism erupted following the government’s May 2015 announcement that internet and text messaging services would be subject to a 10 percent excise duty (see “Availability and Ease of Access”), though at the time of writing, digital activism had not elicited a response from the government.29

Violations of User Rights

A mobile phone monitoring system, known locally as the “spy machine,” was implemented in May 2015, despite repeated concerns over the system’s surveillance capabilities. SIM card registration requirements announced in June 2014 further threatened to violate user anonymity, though the requirements had not been enacted as of mid-2015.

Legal Environment

Malawi has strong constitutional guarantees for freedom of the press and expression, though there are several laws that restrict these freedoms in practice, such as the 1967 Protected Flag, Emblems and Names Act and the 1947 Printed Publications Act, both of which restrict the media from reporting on the president, among other limitations.30 Libel is a criminal and civil offense in Malawi, punishable with up to two years imprisonment if prosecuted as a criminal charge, though most libel cases are processed as civil offences or settled out of court. Otherwise, Malawi’s judiciary is generally regarded as independent and has rendered several significant decisions against the government in recent years, such as its injunction on the implementation of the CIRMS mobile phone surveillance system in 2012 (see “Surveillance, Privacy, and Anonymity”).

While existing legislation pertains primarily to traditional media, the previous administration introduced the draft Electronic Transactions and Management Bill in October 2013 aimed at providing a regulatory framework for the development of ICTs in Malawi, which the current government plans to consider in parliament before the end of 2015. The 2013 draft bill explicitly provides freedom for

---

online public communications but has been criticized for its potential to limit internet freedom.\textsuperscript{31} For example, the bill would require editors of online public communications services to make their personal information—including names, addresses, telephone and registration numbers—available to the public.\textsuperscript{32} The bill would also allow the government to appoint so-called cyber inspectors to “monitor and inspect” websites and report “unlawful activity” to the regulator,\textsuperscript{33} as well as prohibit all types of pornography and penalize offenses with a fine and imprisonment of up to ten years.\textsuperscript{34} There is also a provision that enables the minister of information, in consultation with the regulatory authority, to create any further regulations to support the bill, which some analysts believe is a blank check that can be used to restrict internet freedom in the future.

**Prosecutions and Detentions for Online Activities**

Under Malawi’s former leadership, online journalists were periodically detained and prosecuted for critical articles posted on news websites. Under the new president, there have been no arrests or prosecutions for online activities reported to date.

The last arrest occurred in November 2013 when journalist Justice Mponda, who at the time was correspondent for the online publication *Malawi Voice,*\textsuperscript{35} was arrested for allegedly “intimidating the royal family” in an investigative story about former President Joyce Banda’s connection to the theft of millions of Malawian kwacha from government coffers in a scandal known as “Cashgate.”\textsuperscript{36} Before his arrest, a ruling party official contacted Mponda to take down the story in exchange for MWK 500,000 (US$1,300) but instead had Mponda arrested for extortion when they met for the payment. He was held in detention for four days before being released and charged with “intimidating the royal family,” which was subsequently changed to extortion.\textsuperscript{37} Mponda was later acquitted of all charges in February 2014 due to a lack of reliable evidence.\textsuperscript{38} He had previously been arrested and charged with criminal libel in October 2012 for allegedly insulting former President Banda and publishing false information,\textsuperscript{39} but was acquitted of all charges in February 2013 due to a lack of evidence.\textsuperscript{40} Following the May 2014 elections, current President Peter Mutharika drafted Mponda into his press team, which was seen by some analysts as move to silence him given his history of criticizing presidents.

\textsuperscript{31} Chapter 1: Illegal or restricted content, art.17, Electronic Transactions and Management Bill 2013.
\textsuperscript{32} Chapter 3: Obligations of editors of online contents, art. 24, Electronic Transactions and Management Bill 2013.
\textsuperscript{33} Chapter 2: Cyber-criminality, art. 43, Section 7(a), Electronic Transactions and Management Bill 2013.
\textsuperscript{34} Ten years imprisonment proposed in draft bill, using Zambia’s penalty for such offenses as an example. The draft bill also cites Uganda’s 15-year sentence as an example. See, Chapter 2: Cyber-criminality, art. 45, Electronic Transactions and Management Bill 2013.
\textsuperscript{35} *Malawi Voice* was a frequent target of former President Banda, who reportedly criticized the publication for its “misleading and unbalanced” stories.
\textsuperscript{40} Nkawihe, “Court acquits Malawi online journalist on extortion charge.”
Surveillance, Privacy, and Anonymity

Government surveillance of ICT activities is suspected in Malawi, in large part due to the regulatory authority’s efforts to implement technology known as the Consolidated ICT Regulatory Management System (CIRMS), locally labeled the “spy machine.” Purchased from the U.S.-based company Agilis International for US$6.8 million in 2011, the system was marketed as a tool for MACRA to monitor the performance of mobile phone companies and improve quality of service. Reports, however, indicated that the machine would also allow MACRA to obtain data from telephone operators, including the time, duration, and location of calls, SMS messages sent and received, the type of handset used, and other subscriber details, without judicial oversight. In October 2011, a court issued an injunction against MACRA’s plan to rollout CIRMS, and in September 2012, Malawi’s High Court issued a ruling that banned the implementation of the system altogether. MACRA subsequently appealed the ban at the Supreme Court, which ruled in MACRA’s favor in September 2014, granting the regulator the right to install the system in accordance with the Communications Act. MACRA disclosed that the implementation of CIRMS began in March 2015, which was confirmed by a MACRA official in May 2015. As of mid-2015, no abuses of user privacy have been reported.

By law, service providers are required to hand over user information when presented with a court-issued warrant; however, such legal safeguards have failed to prevent police abuse in the past, particularly under the late-Mutharika regime. For example, in early 2012, when the former Mutharika government suspected a group led by then-Vice President Joyce Banda of scheming to overthrow it, the authorities demanded mobile phone companies hand over transcripts of the group’s mobile phone and SMS communications, which Mutharika apparently planned to use against Banda before his death. No such abuses were reported during the subsequent Banda presidency, and none have been reported under the current President Arthur Peter Mutharika during the coverage period.

Potential restrictions on anonymous communication include SIM card registration requirements announced in June 2014, which were to be implemented by January of 2015, though as of mid-2015, the new requirements have not been enforced.

Intimidation and Violence

Under Malawi’s new leadership, there have been no physical assaults, extralegal detentions, or technical attacks against opposition activists, bloggers, or ordinary users.

Technical Attacks

There were no technical attacks against independent news websites, opposition activists, or ordinary users during the period under review.

46 Interview by Freedom House consultant, May 2015.
Malaysia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>42</td>
<td>43</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 30.1 million

- Internet Penetration 2014: 68 percent
- Social Media/ICT Apps Blocked: No
- Political/Social Content Blocked: Yes
- Bloggers/ICT Users Arrested: Yes
- Press Freedom 2015 Status: Not Free

Key Developments: June 2014 – May 2015

- Dozens of people, including politicians, activists, journalists, and a cartoonist, were questioned or arrested under the Sedition Act, which the government pledged to abolish in 2013 (see Prosecutions and Detentions for Online Activities).

- An April 2015 amendment to the Sedition Act allows the government to block electronic content considered seditious. The maximum jail term increased from three to seven years (see Legal Environment).

- Prime Minister Najib Razak sued popular online news portal Malaysiakini for defamation in 2014, and three other news websites in 2015 (see Prosecutions and Detentions for Online Activities).
Introduction

Malaysia saw positive growth in internet usage in 2014 and 2015, with the Barisan Nasional coalition government pushing forward numerous policies to enable its citizens to become more IT savvy, including cheaper community internet access and affordable mobile phones for rural users. For Malaysians in urban areas, the internet has become a part of life.

This investment has fueled popular political participation and a challenge to the government’s decades-long rule. The internet has become the main tool to enforce checks and balances on government officials, who responded by adapting harsh traditional media laws to curtail criticism online. There were fewer of these measures in the run-up to the 2013 general elections, although critical websites faced cyberattacks and censorship. These abated during the coverage period, though the government has yet to investigate them.

After the opposition eroded the coalition’s parliamentary majority, however, covert cyberattacks appear to have evolved into a legal crackdown on the government’s political opponents. Police arrested bloggers and Facebook users for making sensitive comments online in 2014. Politicians, activists, journalists and academics were also questioned and charged. Worse, the government reneged on its 2013 promise to abolish the draconian Sedition Act and implemented it against dozens of opponents, even strengthening it to allow for official censorship of seditious content. The law was used to arrest dozens of internet users during this review period. In June 2014, Prime Minister Najib Razak filed defamation charges against the popular news portal Malaysiakini. He continued the trend in the first five months of 2015 by suing three other news portals.

Outside the coverage period, in July 2015, the government blocked access to the news portal Sarawak Report for reporting on “unverified contents which could create unrest and threaten national stability, public order and economic stability.” The portal had reported allegations that money linked to the state investment fund ended up in Prime Minister Najib’s bank accounts.

Obstacles to Access

Internet access in Malaysia is considered excellent for the region, despite a digital divide between rural and urban areas. Government policies that promote access are reducing this gap. Mobile phone access is also increasing, providing internet service for many young and rural users. An open market allows fierce competition among providers, resulting in attractive pricing and high quality service.

Availability and Ease of Access

Internet penetration stood at 68 percent in 2014, marking a slight increase from 67 percent in 2013.
Malaysia

This falls short of an ambitious official pledge in 2012 to increase it to 80 percent.\(^5\) Yet those already connected are using the internet more. According to the Malaysian Internet Exchange (MyIX), Malaysia’s internet traffic showed the biggest annual percentage increase in more than a decade in 2013—a 51 percent jump to 349,277 Megabits per second (Mbps) from 230,631 Mbps. Usage is expected to continue to rise in 2014 and 2015.\(^6\)

Internet penetration is concentrated in developed or urban areas. Government statistics show that the highest internet penetration at the end of 2014 was in the highly developed Klang Valley area, which comprises the capital city Kuala Lumpur (71 percent), the nation's most developed state of Selangor (71 percent), and at the administrative capital Putrajaya (89 percent). Penetration remained low in the less populated states of Sabah (43 percent) and Sarawak (41 percent), situated in East Malaysia where most residents belong to indigenous groups. Negeri Sembilan, a state less than an hour’s drive from Kuala Lumpur, had the lowest penetration rate in the country at 40 percent.\(^7\)

The introduction of wireless WiMax technology in 2008 helped bring broadband to regions that are difficult to reach via cable; four WiMax providers were in operation as of mid-2015. Cybercafes also play an important role outside cities. More free Wi-Fi connections are available in many urban spaces including at malls, restaurants, hotels and other tourist spots.

A 2010 National Broadband Initiative expedited broadband and mobile expansion.\(^8\) Around 250 community centers offering broadband internet were established nationwide and nearly 500,000 netbooks were distributed to students and low income citizens in rural and suburban areas in 2011.\(^9\) In 2012, the “1Malaysia” affordable broadband package offered decent broadband speeds for under MYR38 (US$12) per month in five states with lower penetration rates.\(^10\) By 2013, internet centers were expanding to cities,\(^11\) and the government and local councils had introduced schemes to provide free or inexpensive Wi-Fi nationwide.\(^12\) The average monthly cost of fixed internet access is MYR99 (US$30) per month.\(^13\) As of September 2014, there were 437 1Malaysia internet centers nationwide with 433,539 registered users; 120 mini community broadband centers located at Information Departments in under-served areas nationwide; 99 community broadband libraries in rural areas, and 4,803 1Malaysia wireless villages, which bring wireless access to small, remote communities. There were also a total of 30,959 hotspot locations where internet access was available.\(^14\)

Fiber connections are the standard for the fastest household internet connectivity and at present the fastest broadband provider is Time, which can provide connections as fast as 100 Mbps. Other internet service providers such as TM UniFi offer speeds as high as 20 Mbps. Fiber connections are also offered by Maxis, Celcom, and P1.\(^15\)

\(^7\) Malaysian Communications & Multimedia Commission, Communications and Multimedia Pocket Book of Statistics Q3 2014.
\(^12\) Author’s market survey.
\(^13\) Malaysian Communications & Multimedia Commission, Communications and Multimedia Pocket Book of Statistics Q3 2014.
Malaysia

The average internet speed is still comparatively slow, however. A survey by global broadband testing and web-based network diagnostic applications company Ookla in May 2014 found that the average broadband speed in Malaysia was slower than Cambodia and barely ahead of Myanmar. Almost three times slower than Vietnam, Malaysia was ranked 126 out of 192 countries surveyed from May 2013 to April, 2014 at 5.48 Mbps.16

Mobile internet access is easily available, affordable, and popular among young people. Mobile penetration surpassed the country’s total population in 2011 and was approaching 150 percent by late 2014, indicating that some individuals have multiple phone lines.17

In 2013, mobile operators such as Celcom and Maxis introduced 4G LTE wireless broadband service, which is faster than some fiber broadband services, with download speeds up to 75 Mbps. Older 3G and 3.5G connections offer speeds of up to 384kbps and up to 7.2 Mbps, respectively.

Continued growth during the coverage period was due to the spike in the number of smartphone users. The government offered a youth communication package including a MYR200 smartphone rebate for young adults aged 21-30 with a monthly income of MYR 3,000 or less. The government also introduced 25 new smartphones priced around MYR600 into the market.18 The boom in social networking sites such as Facebook, Twitter and Instagram, and data messaging applications such as WhatsApp, WeChat, Viber, LINE and others, have also increased smartphone usage. There was also an increase in IPTV subscribers in 2014, with 742,000 users compared to 658,000 in 2013.

The most recently available government statistics from 2012 showed a slight gender imbalance in access rates, with men representing 56 percent of both internet and mobile users. The most prolific users were aged 20 to 29 (21 percent).

Restrictions on Connectivity

The primary options for broadband internet connectivity in Malaysia are fiber, ADSL, and wireless. Telekom Malaysia, the country’s largest—and formerly state-owned—telecommunications company, retains a monopoly over the fixed-line network.

Malaysia’s internet backbones were operated by Jaring and TMNet during the coverage period.19 The formerly Ministry of Finance-owned Jaring was Malaysia’s first internet service provider, installing its first international satellite leased-circuit at 64 Kbps, connecting Kuala Lumpur to Stockton in the United States. Jaring became a private entity in 2014, but went into liquidation in 2015.20 TMNet is a subsidiary of the now-privatized Telekom Malaysia, Malaysia’s largest internet service provider, and the owner of the nation’s last mile connections. Since there is no local loop unbundling, TMNet enjoys a virtual monopoly of the broadband market.21

18 “Malaysia’s Internet usage rises 51% in 2013, says industry body.”
Malaysia

There are no known cases of any government-imposed restrictions on access to the internet for political reasons during this coverage period, though in the past there were reports of mobile phone jammers being used by the authorities during political rallies. (This was denied by the government.) In recent years, some local authorities have introduced restrictions on cybercafes to curb illegal online activities, particularly gambling, which can result in closure if detected on cafe premises. Select states have capped the number of cybercafe licenses available, making it difficult for legitimate new venues to open.

ICT Market

TMNet and Jaring were the largest ISPs during the coverage period. The largest mobile provider, Maxis Communications, was founded by Ananda Krishnan, who also owns Malaysia’s biggest satellite broadcaster and enjoys close ties to former Prime Minister Mahathir Mohamad. Two new mobile phone providers, YTL Communications and Umobile, have joined the market since 2008. Though ostensibly unrelated to the government, observers believe they benefit from political connections.

As of September 30, 2014, the government had issued 161 Network Facilities Provider licences; 158 Network Service Provider licences; 399 Application Service Provider licences; and 62 Contents Applications Service Provider licences.

Regulatory Bodies

Regulation of the internet falls under the purview of the Malaysian Communications and Multimedia Commission (MCMC), which is overseen by the Minister of Information, Communications, and Culture. The 1998 Communication and Multimedia Act (CMA) gives the information minister a range of powers, including licensing the ownership and operation of network facilities. Similar rules serve as a means of controlling the traditional media, though this has not been documented among internet companies.

The CMA provides for the ministry to appoint the MCMC chairman and three government commissioners, plus two to five commissioners from nongovernmental entities. The current three are all from the private sector. Since 2008, the process for appointing members of the MCMC advisory board has become more transparent and participatory, involving consultations with diverse stakeholders and the inclusion of civil society members on the board. Yet the MCMC remains a driving force in efforts to curtail online speech, including investigations into online portals and bloggers.

Limits on Content

Online content is not restricted in general, but the government is known to have blocked sites perceived as critical. While the digital news media has established a stake in the information market, some news sites have been excluded from government press conferences during the coverage period.

---

Malaysia

*a time when online journalists are also being targeted for rights violations.*

**Blocking and Filtering**

A provision of the CMA explicitly states that none of its wording “shall be construed as permitting the censorship of the Internet.” The Multimedia Super Corridor, an information technology development project, includes a 10-point Bill of Guarantees that promises no censorship to member ICT businesses, though former Prime Minister Mahathir Mohamad told a reporter in 2013 that he regretted that promise.

Generally there are no government blocks or filters on websites except for sites which violate national laws governing pornography. The government has not systematically targeted political content in the past. In 2009, Information, Communications, and Culture Minister Dr. Rais Yatim sought to “evaluate the readiness and feasibility of the implementation of the Internet filter at [the] Internet gateway level,” but backtracked following opposition. In 2013, officials said a total 6,640 sites had been blocked since 2008. However in October 2014, the government said the Malaysian Communication and Multimedia Commission (MCMC) had shut down or blocked at least another 1,400 websites that were deemed inappropriate. No list of affected content is available, but site owners can appeal if mistakenly blocked.

Many government-linked companies and public universities restrict access to Malaysiakini and other sites perceived as politically sensitive.

In 2013, the Federal Department of Islamic Development urged the government to strengthen internet censorship on the grounds that “hundreds of websites on the internet are being used to confuse and weaken those of the Islamic faith.” Google blocked access to the infamous anti-Islamic video, “Innocence of Muslims,” at the MCMC’s request in September 2012. In November 2014, MCMC said that it planned to meet Google and Facebook to seek their help in restricting terrorism content originating from outside the country. However, no terrorism sites were reported to have been blocked during this review period. In July 2015, after the review period ended, the government blocked access to the UK-based whistleblower site Sarawak Report over articles on misallocation of state investment funds, which the government called detrimental to national security.

**Content Removal**


Malaysia

The MCMC periodically instructs websites to remove content, including some perceived as critical of the government, although no such instructions were made publicly in the review period. Requests are generally nontransparent and lack judicial oversight or avenues for appeal.

There have been unpublicized cases of blog owners and Facebook users who have been told to remove their content by the MCMC, especially when the contents touch on sensitive issues involving race, religion and royalty. Religion is particularly sensitive. In 2009, the MCMC directed Malaysiakini to take down two videos containing sensitive religious and political content. When Malaysiakini Editor-in-Chief Steven Gan refused, the MCMC urged the attorney general to prosecute him. As of 2015 the attorney general had yet to pursue the case, although Gan still risks a potential fine of up to MYR 50,000 (US$14,300) and up to one year in prison in the first reported case of its kind.

Media, Diversity, and Content Manipulation

Online news outlets represent an increasingly serious challenge to traditional media, with several among the nation’s most popular websites. In 2013, a judge ordered the home ministry to grant Malaysiakini the right to reapply for a print license. The ministry repeatedly refused to grant the license, and challenged a 2012 appeals court ruling which characterized Malaysiakini’s right to publish a newspaper as fundamental.

The home ministry granted another online outlet, FZ Daily, permission to print a publication in 2013, but deferred the approval required for a license. The daily won the right to challenge the deferral in court in February 2014. The same day, the ministry revoked the publishing permit altogether. In March, the home minister justified the decision on grounds that both FZ Daily and Malaysiakini are “inclined to publish sensational and controversial news.”

Combative political reporting online may have caused the government or its supporters to try to censor a handful of news websites in the lead-up to 2013 elections. The sites were simultaneously targeted by hackers, and the exact nature of the interference remains unclear. At least two outlets filed a complaint with the MCMC, which never responded.

During this review period, while there were no cyberattacks on news portals, some journalists working for them were subjected to informal, inconsistent bans from select government press conferences. An uptick in police reports filed against journalists contributed to a sense of official harassment. In June 2014, Prime Minister Najib and his party Umno sued Malaysiakini for defamation,

---

Malaysia

and three additional news websites in 2015 (see Prosecutions and Detentions for Online Activities). 47

Issues considered potentially sensitive include Islam’s official status, race, royalty, and the special rights enjoyed by Bumiputera, who are ethnic Malays and other indigenous people, as opposed to the ethnic Chinese and Indian minorities. Discussing these topics can lead to prosecution, and some internet users exercise self-censorship.

YouTube, Facebook, Twitter, and international blog-hosting services, as well as other social media platforms, are freely available. In August 2014, the government briefly considered proposals to ban Facebook to curb online abuse. However, this proposal was shot down in October 2014 following complaints from civil society. 48

Expanded internet access has led to the emergence of a vibrant blogosphere. English and Malay are the dominant languages, and many civil society groups, including those representing ethnic minorities, have a dynamic online presence. Prime Minister Najib leads the way with his own blog and almost three million followers on both Facebook and Twitter. 49 Other government representatives are embracing ICTs. The police force has Facebook and Twitter accounts where officers provide updates on policing activities and occasionally respond to accusations of abuse by members of the public. 50

The police chief came under fire in February 2014 for using his tweets to warn off government critics. 51

Some of this engagement is manipulative in nature. Both government and opposition figures are known to pay online commentators, known as “cyber troopers,” to generate favorable content and denigrate their opponents. 52 Since traditional media restrictions caused opposition groups to embrace online platforms relatively early, the government has struggled to catch up. The Barisan Nasional’s dedicated bloggers, Unit Media Baru, deny accepting payment for their efforts. 53 The ruling party, Umno, also maintains paid bloggers. In December 2014, Prime Minister Najib expressed his disappointment when some of them publicly criticized government policies. 54

In 2012, the government admitted paying international public relations firm FBC Media MYR 83.8 million (US$26.5 million) between 2008 and 2010 to boost Prime Minister Najib’s image abroad. 55 Opposition news website Sarawak Report also said Abdul Taib Mahmud, the chief minister in the state of Sarawak, had separately contracted FBC Media for online publicity campaigns. 56 FBC Media, which denied wrongdoing, collapsed in 2011. 57 In February 2015, Sarawak Report said that at least

---

50 Polis Diraja, Facebook page, http://on.fb.me/1yWkBtd.
Malaysia

one former FBC media expert was still in the government’s employment.58

Digital Activism

Online tools have been effective for political mobilization and exposing the government’s grip on traditional media. Social media tools were used effectively by opposition supporters to mobilize following the jailing of opposition leader Anwar Ibrahim for five years in February 2015 for sodomy, a charge his supporters say was politically motivated.59

The Coalition for Free and Fair Elections, which organize for political reform, leveraged online platforms to bring tens of thousands of supporters to the streets during the "Bersih 2.0" and "Bersih 3.0" political rallies in 2011 and 2012, respectively. During the 2013 general election, digital campaigns to get out the vote contributed to a record 80 percent turnout of registered voters, in what observers described as the most closely fought election since independence.60

Violations of User Rights

Two bloggers were jailed in the first quarter of 2015, while two others escaped court action by seeking political asylum elsewhere. A number of civil society activists, politicians, and a journalist have been hauled up over their online remarks. The police continue with their crackdown, armed with the government’s promise of a sedition law with harsher penalties, all creating a chilling effect on social media users. At the same time, there were fewer distributed denial-of-service (DDoS) attacks targeting alternate news portals and opposition websites.

Legal Environment

Malaysia’s constitution provides citizens with “the right to freedom of speech and expression,” but allows for limitations on this right. While some court decisions have disappointed freedom of expression advocates,61 others show more independence. The government exercises tight control over online as well as print and broadcast media through laws like the Official Secrets Act and the Sedition Act. Violations are punishable by fines and several years in prison. In November 2014, Prime Minister Najib reneged on his reform vows made in 2013 to abolish the Sedition Act. In fact, the government widened the scope of the sedition law with new amendments in April 2015, allowing the government to block electronic content considered seditious,62 and strengthening penalties. Under the amended law, the penalty for sedition is now seven years in prison, up from three years previously. A new provision allows for a penalty of up to 20 years for seditious activities that result in

---

Malaysia

physical harm or destruction of property.  

Defamation is a criminal offence under Sections 499 to 520 of Malaysia's penal code. Media outlets benefit from stronger privileges under the Defamation Act 1957 if they can prove allegedly libelous content is accurate and was published without malice; lacking this protection, bloggers risk punitive damages.

In 2012, parliament passed an amendment to the 1950 Evidence Act that holds intermediaries liable for seditious content posted anonymously on their networks or websites. This would include hosts of online forums, news outlets, and blogging services, as well as businesses providing Wi-Fi services. The amendment also holds someone liable if their name is attributed to the content or if the computer it was sent from belongs to them, whether or not they were the author. The legal change was pushed through hurriedly, but garnered significant public backlash after its passage, which failed to prevent it going into effect. No implementation has been reported.

The government has also pursued prosecutions for online content based on the CMA's broadly worded Section 211, which bans content deemed “indecent, obscene, false, threatening, or offensive,” and Section 233. Amendments to the CMA and the related Communications and Multimedia Commission Act (CMCA) 1998 are expected to be tabled in October, including measures to curb “social media misuse, that infringe, among others, on religious and racial sensitivities, or for recruitment of terrorists.” Critics say the intention is to stop online criticism against the government.

Prosecutions and Detentions for Online Activities

During this review period, police arrested numerous online users under the sedition law for remarks against the government and its policies, royalty, or Islam. Some also faced charges for allegedly stoking racial tensions in the country through their tweets or Facebook postings. Among the more prominent arrests under the Sedition Act during this review period are the following:

- In June 2014, Facebook users Gopinath Jayaratnam and Hidayat Muhamad were charged for allegedly insulting Islam and Hinduism. Their cases are pending.

Malaysia

- In August 2014, a 15-year-old student was investigated for “liking” a Facebook page called “I Love Israel.” No further action has been taken against him.76

- On September 2, 2014, academic Dr. Azmi Sharom was charged over his online article in a news portal relating to a political crisis in the country. His trial is ongoing. He faces a jail term of up to seven years or maximum MYR 5,000 (US$1,040) fine or both if found guilty.77

- On September 3, 2014, opposition politician David Orok was charged with sedition for allegedly insulting Islam and the Prophet Mohamed on his social media page.78

- On February 5, 2015, lawyer and activist Eric Paulsen was arrested over a tweet stating that the Malaysian Islamic Development Department (Jakim) was spreading extremism through their Friday sermons. He is now out on bail, but his trial is ongoing.79 Paulsen was detained for the second time for sedition on March 22, 2015, but released without charge after questioning.80

- A handful of political leaders were questioned over tweets criticizing opposition leader Anwar Ibrahim’s five year jail sentence on sodomy charges in February.81

- Popular cartoonist Zunar was arrested and charged with sedition over his pro-Anwar tweet which questioned the Malaysian judiciary. He was released on bail but the charge is pending.82

- On March 30, 2015, the police arrested three editors from The Malaysian Insider news portal, along with the publisher and the chief executive the following day, over a report on Islamic criminal laws.83 The police investigation centered on complaints that the news portal had carried a false report about the Malay Rulers, hereditary monarchs of the nine Malay states, objecting against the implementation of Islamic laws in a state in Malaysia. The rulers denied objecting, and the five journalists were held overnight for questioning before being released without charge. The news portal subsequently apologized for the report, which was attributed to an unnamed source.84

The government separately implemented the penal code to punish online commentators. On January 19, 2015, pro-opposition blogger Yusuf Siddique Al-Suratman was jailed for two years under Section 505 (b) of the penal code on a charge of causing fear and public alarm in a 2013 blog post.

about a police anti-terrorism operation. On January 11, 2015, a couple was arrested for disseminating false information about flooding via WhatsApp, and were remanded under Section 233 of the Communications and Multimedia Act 1998. No further action was taken against them. In February 2015, Ismail Sabri Yaakob, then minister of agriculture and related industries, was asked to give a statement to police after calling for Malay consumers to boycott Chinese traders on Facebook. He did not face further action during this review period.

Trials related to sensitive comments made in the social media platform during the previous coverage period were ongoing. Police outside Kuala Lumpur detained a Facebook user they identified as “Man Namblast” in February 2014 for allegedly posting seditious remarks about Hindus. He was charged with sedition on June 19. His trial is ongoing. On May 6, 2014, opposition politician Teresa Kok was charged with sedition for allegedly insulting Islam and the nation’s leaders, four months after sharing an 11-minute video that used invented Chinese New Year predictions to satirize government policies. The video sparked outrage among a group of Muslim NGOs, who staged protests saying Kok was using politics to fan racial hatred. One group slaughtered chickens, smeared the blood on a poster of opposition leaders, and offered a financial reward for slapping Kok in retaliation for the video. Kok’s trial was pending during this coverage period. During the review period, Facebook users Alvin Tan and Ali Abdul Jalil had also left the country to seek asylum elsewhere. They were both facing jail terms in Malaysia for charges under the sedition law over allegedly sensitive remarks posted in the social media.

Politically motivated defamation suits seeking damages disproportionate to the offense have become another threat to online expression since a landmark 2007 blogger prosecution by a government-linked newspaper. In August 2012, a Kuala Lumpur court sentenced blogger and opposition People’s Justice Party member Amizudin Ahmat to three months in jail on charges of contempt for blogging about Dr. Rais Yatim, Malaysia’s information and culture minister, after being banned from doing so in a 2011 defamation ruling against him. He lost his appeal in January 2015 and was sent to prison.

In June 2014, Prime Minister Najib filed a defamation suit against Malaysiakini for two allegedly defamatory articles published in May that compiled readers’ comments. The case had not been heard as of May 2015. Najib subsequently filed suit against two other news portals, the opposition party

Malaysia

organ Harakah Online and the pro-opposition Media Rakyat, claiming that they had defamed him. The two charges against Media Rakyat also name two opposition lawmakers. If defeated, the websites could be forced to pay the prime minister significant damages.

Separately, Malaysiakini journalist Susan Loone was arrested on September 4, 2014 over an article which allegedly defamed the police. Her article stated that an arrested opposition lawmaker was treated like a criminal by the police; the lawmaker himself said that he was well-treated under custody. She was released the next day, and so far no charges have been filed.

In March 2015, journalist Aisyah Tajuddin and independent radio station BFM were hauled up for mocking Islam in a video posted in YouTube. BFM Radio then removed the video from its YouTube page, but Aisyah is now being investigated by police for blasphemy, and could face up to a year in jail if convicted. She also received death and rape threats over the video. There were no developments in the investigation as of May 2015.

Surveillance, Privacy, and Anonymity

Real-name registration is not required for participation in Malaysia’s blogosphere, nor is it required to use a cybercafe. Beginning in 2007, all mobile phone owners, including the roughly 18 million customers using prepaid service at the time, were required to register as part of an effort to decrease rumor mongering. The rule appears to have been weakly enforced.

The extent of government surveillance of ICT content is not known, but privacy protections are generally poor. In 2008, the MCMC formed a panel composed of representatives from the police, the attorney general’s office, and the Home Ministry to monitor websites and blogs. Although it still appears to be active, it has not publicly intervened in internet freedom issues. Court documents indicate that police regularly gain access to the content of text messages from telecommunications companies, sometimes without judicial oversight. SOSMA, which allows for the interception of communications without a judicial order in poorly defined security investigations, also contains scope for abuse.

The Malaysian Personal Data Protection Act 2010, which regulates the processing of personal data in commercial transactions, came into effect in November 2013. The law makes it illegal for commercial organizations to sell personal information or allow third parties to use it, with penalties up to MYR 100,000 (US$27,400) or one year imprisonment. Federal and state governments are exempted from the law, as is data processed outside Malaysia. But the act requires that information about M-

Malaysia

Malaysians be stored locally, and limits conditions under which the data can be transferred abroad. No implementation was reported during the coverage period.\footnote{Anupam Chander and Uyen P. Le, “Breaking the Web: Data Localization vs. the Global Internet,” (UC Davis Legal Studies Research Paper No. 378, Emory Law Journal, April 2014) \url{http://bit.ly/18a2KuA}.}

In 2013, the University of Toronto-based research group Citizen Lab reported detecting software known as FinFisher, described by its distributor Gamma International as “governmental IT intrusion and remote monitoring solutions,” on 36 servers worldwide, including one in Malaysia.\footnote{Morgan Marquis-Boire et al., “You Only Click Twice: FinFisher’s Global Proliferation,” Citizen Lab, March 13, 2013, \url{http://bit.ly/1qoVFD}.} The software potentially allows the server to steal passwords, tap Skype calls, or record audio and video without permission from other computers, according to Citizen Lab. The same month, the Malaysian Insider documented FinFisher’s presence in Malaysia, based on a New York Times report.\footnote{Boo Su-Lyn, “Malaysia uses spyware against own citizens, NYT reports,” The Malaysian Insider, March 14, 2013 \url{http://bit.ly/1E52Ssf}; The original New York Times article: Nicole Perlroth, “Researchers Find 25 Countries Using Surveillance Software,” The Business of Technology (blog), The New York Times March 13, 2013, \url{http://nyti.ms/1G2XSOv}.} In response, the MCMC threatened the site with a fine of up to MYR 50,000 (US$15,200) or one year imprisonment for false reporting under the CMA. No charges were filed against the website or its staff. However, Citizen Lab subsequently reported they had further identified “a Malaysian election-related document” they characterized as a “booby-trapped candidate list” containing surveillance spyware.\footnote{“Short Background: Citizen Lab Research on FinFisher Presence in Malaysia,” Citizen Lab, May 2013, \url{http://bit.ly/1zNT7Bo}.} Because the spyware is only marketed to governments, “it is reasonable to assume that some government actor is responsible,” the group concluded. A separate Citizen Lab report published in 2014 said a Malaysian government agency was a “current or former user” of Remote Control System spyware marketed by the Milan-based Hacking Team.\footnote{Bill Marczak et al, “Mapping Hacking Team’s ‘Untraceable’ Spyware,” Citizen Lab, February 17, 2014, \url{http://bit.ly/1kPDo0Y}.}

Intimidation and Violence

Physical violence sporadically affects traditional and online journalists in Malaysia.\footnote{CPJ, “Journalists assaulted, detained during rally in Malaysia,” April 30, 2012, \url{http://cpj.org/x/4b4a}.} No incidents were documented during the coverage period of this report.

Technical Attacks

Independent online news outlets and some opposition-related websites have faced intense DDoS attacks, which force sites to crash sites by overloading the host server with requests for content, often at moments of political importance. Some observers believe such attacks are either sponsored or condoned by Malaysian security agencies, since they often align with government priorities. Malaysiakini was one of many sites reporting on the opposition which were subjected to an apparently coordinated assault before the May 2013 elections.\footnote{Human Rights Watch, “Malaysia: Violence, Cyber Attacks Threaten Elections,” May 1, 2013, \url{http://bit.ly/1Ezugqi}; Shawn Crispin, “In Asia, Three Nations Clip Once-Budding Online Freedom,” in Attacks on the Press, Committee to Protect Journalists (New York: Wiley, February 2013), \url{http://bit.ly/1wxd40x}.} Though attacks are known to continue, no severe or crippling incidents were reported by news portals and opposition websites during this review period.

\begin{footnotesize}

106 “Short Background: Citizen Lab Research on FinFisher Presence in Malaysia,” Citizen Lab, May 2013, \url{http://bit.ly/1zNT7Bo}.
\end{footnotesize}
Mexico

Key Developments: June 2014 – May 2015

- In 2014 and early 2015, Mexico continued to be one of the most hostile environments in the world for online journalists and bloggers, who were subjected to retaliatory violence from drug cartels, organized crime, and public officials. In this period, one online citizen journalist and at least seven other journalists were killed (see Intimidation and Violence).

- The Federal Telecommunications and Broadcasting Law, which was approved on July 14, 2014, may potentially increase ICT competition and affordability. However, certain provisions in the law could constitute a significant breach of users’ privacy (see ICT Market and Surveillance, Privacy, and Anonymity).

- A ruling by the Federal Institute of Access to Information and Personal Data Protection (IFAI)¹ may set a precedent for users to request that search engines remove results that violate their privacy or harm their reputation (see Content Removal).

- Online journalists continued to be victims of serious cyberattacks. In this period, six major cyberattacks on journalists and media publications took place (see Technical Attacks).

---

¹ In May 2015, this institute changed its name to the National Institute of Transparency, Access to Information, and Personal Data Protection (INAI).
Mexico

Introduction

Internet access has improved in recent years, and new legislation has already begun to promote diversity in Mexico's highly concentrated information and communications technology (ICT) market. Nevertheless, internet freedom is severely limited by one of the highest levels of violence against journalists in the world. Online journalists, bloggers, and social media activists often risk their safety to report on local crime and corruption. Using the tense security situation and the war on drugs as justification, the state has ramped up its legal surveillance powers through a recent telecommunications reform.

Online publications have suffered severe cyberattacks, journalists have received death threats, and at least one online journalist was murdered during the coverage period. Although the June 2012 Law to Protect Human Right Defenders and Journalists allows federal authorities to investigate attacks against journalists and human rights defenders and to provide them with protection, it has suffered from inadequate enforcement and delays in responding to requests for protections.¹

In this climate of insecurity, the government expanded its powers of surveillance by passing the Telecommunications Law in July 2014. This law requires internet service providers (ISPs) and mobile providers to store user data for at least two years and to provide detailed communication records to police without a judicial warrant. Meanwhile, recent reports of Mexican government contracts with the Italian surveillance company Hacking Team suggest that state surveillance is widespread.

Mexico has experienced dramatic improvements in both internet penetration and quality of access over the last 25 years; for example, average connection speeds increased from 1.08 Mbps in 2007 to 4.5 Mbps in 2015.² Nevertheless, the country still faces challenges in its quest to extend internet access to all citizens. Regional disparities create a stark digital divide, in which individuals living in large cities have much greater access to affordable internet service than those in smaller towns and more remote areas.

The Mexican ICT market has historically been characterized by extremely high market concentration, which has contributed to high prices and reduced access. Through the Telecommunications Law, the government has sought to reduce this concentration by curbing the dominance of América Móvil, which owns 80 percent of landlines and 70 percent of wireless internet subscriptions in Mexico and is headed by Carlos Slim, one of the world's richest individuals.³ Although the law empowered the new regulatory body, the Federal Telecommunications Institute (IFETEL), to begin to break up Mexico's highly concentrated telecommunications market, six private companies still dominate the industry, offering broadband service at prices beyond the reach of many low-income citizens.

Obstacles to Access

Implementation of the new Telecommunications Law has opened the market and started to reduce concentration of the sector. This development has the potential to increase availability and ease of access to the internet. At the same time, the government has launched its plan to use the national fiber-optic network, owned by the Federal Commission of Electricity, to expand internet service throughout the country. So far, however, the country still suffers from a huge digital divide between the north and south of the country.

Availability and Ease of Access

Internet penetration in Mexico has increased significantly over the past five years. According to data from the International Telecommunications Union (ITU), internet penetration reached 44 percent in Mexico in 2014, compared to 43 percent in 2013 and just 26 percent in 2009. Although access has continued to grow each year, the rate of this growth has decreased slightly in recent years.

New legislation and government initiatives may significantly reshape the telecommunications industry and increase access, but the real-world impact of these relatively new policy changes still remains to be seen. The Telecommunications Law, passed in July 2014, aims to reduce market concentration in the sector, which could increase access by increasing competition and reducing the very high prices for mobile and internet services in the country.

Meanwhile, following advice from civil society groups, the government has announced plans to use the national infrastructure of the Electricity Federal Commission (CFE) to provide improved internet access across the country. In December 2014, as part of the constitutional reform in telecommunications, the Federal Electricity Commission granted the state company Telecomm (Telecommunications of Mexico) use of a 40,000 kilometer-long fiber-optic cable network. Telecomm hopes to use and expand this infrastructure, which can transmit data, video, and voice communications, with the goal of expanding internet access to 98 percent of homes.

As of early 2015, however, Mexico continued to suffer from limited access, and the digital divide between the north and south has widened. While the proportion of homes with access to the internet grew from 30.7 percent in 2013 to 34.4 percent in 2014, the proportion of homes with access to internet in some of the poorest states was unchanged. In 2014, more than half of homes had access to the internet in Nuevo Leon, Mexico City and Baja California, while only one in ten had access to the internet in Chiapas and Oaxaca.

8 Instituto Nacional de Estadística y Geografía, “Módulo sobre disponibilidad y uso de las tecnologías de la información en
Mexico

Such limited and disparate connectivity rates are also evident in the relatively small percentage of internet users with broadband access. According to the National Institute of Statistics and Geography (INEGI), 34.4 percent of Mexicans had household internet access as of 2014. Although the number of Mexicans with broadband subscriptions has increased over the past decade, growing from 0.4 percent in 2003 to nearly 12 percent in 2014, Mexico still falls significantly below the broadband penetration rates of other OECD countries, which have an average rate of approximately 27 percent. In Mexico where the minimum wage is US$150 per month, the high price of broadband service, which can range from US$26 to US$100 per month, is a significant factor in the country’s low broadband penetration rate.

Internet cafes and the availability of internet at the workplace and schools have partially ameliorated the disparities in internet use between socioeconomic groups. Although 58 percent of all computer users in Mexico access the internet from home, in 2014, the remaining 42 percent of computer users (nearly 18 million) sought access from other places, such as internet cafes or computers at their workplace.

The emergence of mobile technologies has also increased internet access in Mexico. Notably, the mobile broadband penetration rate, which grew nearly 19 percent between December 2013 and June 2014 to reach a penetration rate of roughly 40 percent, far surpasses the penetration rate of fixed household broadband subscriptions, which grew 3 percent in the same period to a current penetration rate of 12 percent. Although Mexico had the third-highest growth in mobile broadband penetration among OECD countries between December 2013 and June 2014, it still lags well behind most other OECD countries in terms of mobile internet penetration.

Mobile phone access is significantly more widespread in Mexico than is internet use, with the ITU reporting a mobile penetration rate of 83 percent (about 102 million users) as of 2014. However, this rate still puts the country behind other countries in the region. As of December 2014, an eMarketer study estimated that there were 29 million smartphone users in Mexico. The prevalence of smart-

---

9 Instituto Nacional de Estadística y Geografía, “Módulo sobre disponibilidad y uso de las tecnologías de la información en los hogares, 2014.”
14 Based on statistics regarding Mexico’s population and internet penetration, it is possible to calculate that there are roughly 43 million internet users in Mexico; of these, 42 percent or nearly 18 million do not have internet access at home and must seek it outside the home. Instituto Nacional de Estadística y Geografía, “Estatísticas sobre la disponibilidad y uso de las tecnologías de la información en los hogares, 2014.”
15 Instituto Nacional de Estadística y Geografía, “Estatísticas sobre la disponibilidad y uso de las tecnologías de la información en los hogares, 2014.”
phones is due in part to a recent drop in prices for mobile phone use,\textsuperscript{20} the increasing availability of smartphones, and promotions that narrow the price gap between basic phones and smartphones.\textsuperscript{21} Mexico is reportedly home to the second largest smartphone market in Latin America, following Brazil, and the tenth largest in the world as of 2013.\textsuperscript{22}

### Restrictions on Connectivity

There have not been any recorded activities or public incidents related to government imposed restrictions on ICT connectivity or restrictions on access to particular social media or communications applications during the period of this report. Article 190 in the recently passed Telecommunications Law, however, authorizes the “appropriate authority” within the Mexican government to request the suspension of telecommunications service in order to “halt the commission of crimes.”\textsuperscript{23}

Civil society groups successfully rallied to remove wording from earlier drafts of the Telecommunications Law that would have allowed the government to temporarily block telecommunications signals “in events and places critical to the public and national security.”\textsuperscript{24} Although the version of the law that was approved narrowed the parameters for blocking telecommunications signals in comparison with the proposed draft of the law, there are still concerns that authorities could abuse these provisions to limit expression in critical moments. The United Nations Special Rapporteur on Freedom of Expression, along with other international organizations, has stated that shutting down entire parts of the communications system cannot be justified under human rights law.\textsuperscript{25}

Although the majority of the backbone infrastructure in Mexico is privately owned, the state-owned company Telecomm has taken on greater control of the infrastructure, after taking over the fiber-optic infrastructure from the Federal Electricity Commission.\textsuperscript{26} Mexico has only one Internet Exchange Point (IXP), set up by KIO Networks in April 2014. Experts say that this IXP may increase efficiency and reduce costs for Mexican ISPs by helping to manage traffic across networks.\textsuperscript{27}

### ICT Market

In June 2013, the president approved a constitutional amendment aimed at reforming the telecommunications sector.\textsuperscript{28} Through that reform, the government hoped to increase competition via

\textsuperscript{20} In May 2011, COFETEL ordered telecom firms to reduce interconnection fees between landlines and mobile phones to a more affordable level. The fees were dropped to 0.39 pesos (US$0.03) for mobile phones. The decision was later affirmed by the Supreme Court. See: “Cofetel reduces fixed line interconnection rate,” TeleGeography, June 10, 2011, http://bit.ly/1LKQyVv.


\textsuperscript{26} Peralta, “Telecomm venderá conectividad de fibra óptica en 2015.”


asymmetric regulation, to force divestment of companies with a monopoly on telecommunications, and to lighten restrictions on foreign investment. In July 2014, the government finally approved secondary legislation allowing the recently created Federal Institute for Telecommunications (IFETEL) to launch a process to reduce the market dominance of two América Móvil companies: Telcel in the mobile market and Telmex in the fixed segment.

Prior to the reform, six private companies controlled Mexico’s mobile phone sector, with one company eclipsing all others in market dominance. Carlos Slim’s América Móvil, which counts both Telmex and Telcel as subsidiaries, dominated the ICT landscape with 80 percent of landline subscriptions and 70 percent of the wireless market in 2013. The top competitor in fixed line subscriptions, Axtel, only accounted for 6 percent of that market, while the top competitor in wireless connections, Movistar, claimed 20 percent of wireless subscriptions.

Mexico’s Telecommunications Law prohibits companies from controlling more than 50 percent of the market share. In March 2014, IFETEL, the new regulator, declared América Móvil a dominant company, indicating that it violated antitrust standards under the law. In response, América Móvil preemptively started selling assets to comply with the new regulations.

Over the past year, IFETEL has continued to issue decisions targeted at reducing América Móvil’s dominance in the market. In an important step that has the potential to reduce costs and obstacles to calling between phone networks, IFETEL determined that the company must eliminate mobile roaming charges and fees for receiving incoming calls from rival providers on Telcel’s network. Under new regulations, América Móvil also initiated steps to allow other telecommunications providers to use its platform, and after a long legal dispute, América Móvil and Axtel reached an agreement for the latter to offer mobile phone services on América Móvil’s network. Through this agreement, Axtel will become the first virtual mobile network leasing space from Americas Movil network unit Telcel.

Although it is early to assess the overall impact of the Telecommunications Law on market concentration, competition, and prices, the initial developments seem to bode well for ICT competition in Mexico. In January 2015, for example, U.S.-based carrier AT&T closed a $2.5 billion deal with the purchase of Iusacell, the third largest Mexican carrier from Grupo Salinas, marking the entrance of U.S. companies into the Mexican market and increasing competition for América Móvil.

Regulatory Bodies

In 2013, the government established a new autonomous regulatory apparatus known as the Federal

---

Mexico

Telecommunications Institute (IFETEL) as part of a constitutional reform, in order to increase transparency of media regulation. IFETEL has the legal mandate to act as an antitrust body, protecting the industry against monopolistic practices. Its abilities were put on hold, however, until secondary legislation was passed in July 2014. Though it could still make rulings, the lack of secondary legislation was grounds for dominant companies to appeal the regulator’s rulings before a court.

After secondary legislation was approved in July 2014, however, IFETEL began acting on its mandate to unilaterally punish non-competitive practices through the withdrawal of corporations’ licenses, the application of asymmetric regulation, and the unbundling of media services—stipulations that may portend a dramatic change in the Mexican ICT landscape. The most notable step taken by IFETEL was the declaration that América Móvil and Televisa were dominant companies. This action indicates positive changes in Mexico’s telecommunications market, especially if IFETEL can continue to remain independent from political and corporate interests.

Limits on Content

There is no evidence of blocking or filtering of online content in Mexico, but the government has increased requests to social media companies to remove content. Meanwhile, harassment and physical violence contributed to self-censorship among journalists and online activists, although many have continued to risk physical danger in order to write about crime and corruption. Public officials and private actors also used harassment and economic constraints to manipulate the media environment. In March 2015, for example, a team of online investigative journalists was fired after publishing a story about government corruption.

Blocking and Filtering

No evidence has been documented that the government or other actors blocked or filtered internet and other ICT content. Facebook, Twitter, YouTube, and international blog-hosting services are freely available in Mexico and have enjoyed steady growth in recent years.

Content Removal

The Mexican government does not systematically request content removal. Facebook did not register any content removal requests for 2014, and Twitter registered two government agency requests for content removal, with which it did not comply. Although there is little legislative framework for intermediary liability, the existing legislation offers some protections from liability for ISPs in cases of copyright infringement. A crucial new ruling from the Federal Institute of Access to Information and Personal Data Protection (IFAI), now known as the INAI after a recent name change, may indi-

40 This was the name of the institute at the time of the ruling. However, in May 2015, the institute changed its name to the National Institute of Transparency, Access to Information, and Personal Data Protection (INAI).
Mexico

cate greater liability for search engines if they do not comply with requests to remove sensitive personal information from their search results.

In July 2014, Carlos Sanchez de la Peña, a businessman whose family had extensive dealings in the transport sector, sent an appeal to Google Mexico asking it to remove three links from search results on the grounds that these links, which included criticisms of his family’s business dealings, constituted an affront to his honor and privacy. Google Mexico dismissed the request on jurisdictional grounds, at which point Sánchez petitioned the IFAI to force Google Mexico to remove the links. In January 2015, the IFAI conceded to Sánchez’s request and ordered Google Mexico to remove the links under threat of sanction. In its decision, the IFAI, following in the footsteps of several so-called “right to be forgotten” cases, argued that individuals had the right to demand that the search engine remove search results that might violate their privacy.

Civil society groups have expressed serious concern that the ruling could set a precedent for intermediary liability and censorship. They have also raised issue with the type of content that was censored. Although Sanchez characterized the links as defamatory and a violation of his personal privacy, civil society groups have argued that the links—which included a journalistic investigation in the media outlet Revista Fortuna about fraud—had public interest value. Both Google and Revista Fortuna, represented by the digital rights group R3D, have challenged the resolution, and Google has succeeded in obtaining an injunction. Mexican courts have not yet ruled on the right to be forgotten, although the legal challenges presented to the IFAI ruling could provide them with an opportunity to do so.

Media, Diversity, and Content Manipulation

While there is no legislation that restricts internet content, local officials have often been accused of manipulating online content in their favor, or of harassing or otherwise attempting to intimidate journalists to keep them from writing about issues of local corruption and crime.

The climate of violence and harassment towards the media contributes to significant self-censorship. In some states heavily afflicted by violence, the local media will simply not report stories about drug trafficking or drug-related violence. An investigation by the MEPI Foundation, a Mexican non-profit focused on promoting investigative journalism, found that in a survey of citizens who live in 15 high-crime cities, eight out of ten respondents said that they knew that local media would not report on crime in their area.

In several cases, evidence suggests that public officials also attempted to manipulate media content by exerting pressure on media outlets to fire reporters who are critical of the government. On June 25, 2014, for example, the Chihuahua-based reporter Gabriel Ortega denounced the TV station Azteca Chihuahua, claiming that the station had fired him after he used his personal Facebook account

---

44 Susana Guzmán, “Google litia contra el Ifai por el ‘derecho al olvido’” [Google litigates against the IFAI over the right to be forgotten], La Razon, April 28, 2015, http://bit.ly/1hPm4CB.

577
to criticize both the state and the city governments.\footnote{Periodistas en Riesgo, “Denuncia reportero espionaje virtual y despido,”[Reporter claim he was spied electronically and fired] June 25, 2014, accessed April 15, 2015, \url{http://bit.ly/1MVbf02}.} In a case that generated far more media attention in March 2015, MVS, an independent radio station, terminated its contract with the Aristegui Noticias team, a group of investigative journalists that used to run stories on the MVS radio station. MVS said that the dismissal was related to the involvement of members of the investigative team in a new website Méxicoleaks, which encourages whistleblowers to come forward anonymously. The company accused the journalists of using the MVS brand in association with the Méxicoleaks project without permission.\footnote{Elisabeth Malkin, “In Mexico, Firing of Carmen Aristegui Highlights Rising Pressures on News Media,” The New York Times, March 27, 2015, \url{http://nyti.ms/1FDE7yz}.}

Many critics believe that the real reason for the termination, however, was a reaction to a controversial report published online by the Aristegui Noticias team two months earlier that investigated a luxurious residence in Mexico City owned by President Enrique Peña Nieto’s family.\footnote{“La casa blanca de Enrique Peña Nieto (investigación especial),” [The white house of Enrique Peña Nieto (special investigation)] Aristegui Noticias, November 9, 2014; accessed April 17, 2015, \url{http://bit.ly/1xc1FVN}.} The proximity between the publication of the story and the dismissal of the entire Aristegui Noticias team raised suspicions about the role of governmental pressure on MVS. Edison Lanza, the Special Rapporteur of Freedom of Expression at the Interamerican Commission of Human Rights criticized the firing saying that it might be “a subtle form of censoring a critical voice.”\footnote{Associated Press, “Depido de Aristegui huele a censura: CIDH,” El Economista, March 23, 2015, \url{http://bit.ly/1LKw8Rm}.} After MVS terminated the contract, the team continued to publish stories on their website aristeguinoticias.com.

Online trolls have targeted both online and print journalists through Twitter and other social media, and some reports suggest that some government officials or powerful figures regularly employ commentators or bots in order to manipulate online debate.\footnote{Alberto Nájar, “¿Cuánto poder tienen los Peñabots, los tuiteros que combaten la crítica en México?,” BBC Mundo, March 7, 2015, \url{http://bbc.in/1KG9b8X}; Erin Gallagher, “Tracking The Mexican Botnet: Connecting the Twitterbots,” Revolution News, March 18, 2015, \url{http://bit.ly/1FS4CxF}.} The news portal Sin Embargo reported on October 8, 2014 that it was subject to attacks by anonymous users, thought to be bots, posting comments on the website accusing the editors of corruption.\footnote{Periodistas en Riesgo, “Ataque cibernético a portal Sin Embargo,” [Cyberattack to Sin Embargo portal] October 8, 2014, accessed April 15, 2015, \url{http://bit.ly/1k15p2X}; “Bots lanzan ataque masivo contra SinEmbargo, defienden al gobernador Aguirre,” Sin Embargo, October 8, 2014, \url{http://bit.ly/2tedx}.} Before the threats, Sin Embargo had run a story critical of local officials.

After publishing an article on the online media platform Aristegui Noticias in February 2015 criticizing the detention of human rights defender Pedro Canché, journalist Lydia Cacho said that she faced attacks from trolls accusing her of accepting money from public officials.\footnote{Periodistas en Riesgo, “Campaña de desprestigio contra Lydia Cacho,” [Defamation campaign against Lydia Cacho] February 10, 2015, accessed April 15, 2015, \url{http://bit.ly/1lbYVQP}.} Trolling campaigns seem to be a regular form of attack against independent online journalists and bloggers in Mexico. The map of press freedom violations, “Journalists at Risk,” shows at least two other major cases of trolling attacks against @MrCruzStar, an online activist in Tamaulipas,\footnote{Periodistas en riesgo, “Campañas de difamación en contra de reporteros ciudadanos de ReynosaFollow,” July 22, 2014, \url{http://bit.ly/1Fsk19j}.} and Sandra de los Santos, a reporter for the online media outlet Chiapas Paralelo.\footnote{Periodistas en riesgo, “Campaña de difamación contra periodista Sandra de los Santos,” April 2015, \url{http://bit.ly/1JyNRFh}.}

Economic constraints influence the diversity of media in Mexico. Scarce funding and a lack of inter-
est in online advertising create challenges for individuals and nonprofits seeking to establish sustainable online outlets in Mexico. Reliance on public advertising renders independent media vulnerable to manipulation of content or closure due to lack of funding, although it is the former that appears to be the more pernicious of the two trends. In Puebla, for example, independent media organizations say the state government uses a combination of state, municipal, and university advertising as a way to control the editorial independence of local media. According to the editor of La Jornada de Oriente, this mechanism of control has forced the shutdown of at least six online and print media outlets.

A study by the World Association of Newspapers and the Fundar Center for Analysis and Investigation interviewed Mexican media managers and found that local media organizations frequently depended on governmental advertising for 50 percent or more of their budget. For the second year, the current administration reduced the budget for public advertising by 18 percent. Nongovernmental organizations (NGOs) say that the allocation of this budget is less than transparent and opens the possibility of governmental control of media. For some media organizations that depend on governmental advertising, a reduction in public funding might mean shutting down business.

Despite such challenges, however, financially independent digital media outlets are appearing in Mexico, creating a new ecosystem of news options. These independent outlets, such as Paralelo, an outlet created by freelance and local journalists in Chiapas, bring new voices to the public debate. Another new digital media venture, Animal Político, a popular site that claims more than one million followers on Facebook, is successfully experimenting with alternate forms of financing. In order to raise revenue for the site without compromising content based on advertisers’ political leanings, Animal Político is practicing brand journalism, offering social media consulting and digital content to private companies. Additional financing is derived from syndicated content, private sponsorships, and a new outlet named Animal Gourmet. Other digital media outlets have emerged in Mexico City, Puebla, and Oaxaca.

The social media landscape in Mexico is also vibrant. Mexico has the second largest community of Facebook users in Latin America after Brazil—and the fifth largest in the world—with an estimated 40 million users, which represents over 90 percent of all internet users. It also has the second highest Twitter penetration in Latin America with 12 percent of internet users regularly accessing a Twitter

---

56 “México,” in Article VIII, Control estatal de los medios de comunicación,” 60.
59 The website can be found at: [http://www.chiapasparalelo.com](http://www.chiapasparalelo.com).
61 Tania Lara, “Popular Mexican news site Animal Político seeks to eliminate dependence on government advertising,” Journalism in the Americas Blog.
account. The number of internet users in Mexico with Twitter accounts ballooned in recent years, growing from 3.5 million in 2012 to 7.7 million in 2014.

Articles 145 and 146 of the Telecommunications Law establish protections for net neutrality. However, net neutrality has reemerged as a contentious issue with Facebook’s announcement that it is hoping to introduce Internet.org, a zero-rating platform that grants the user access to certain online applications, in Mexico. Zero-rating programs, which are operated by most of the major mobile providers, have generated significant debate. Facebook argues that limited access is better than no access and that this program will introduce millions to important social, health, and political resources on the internet. Critics, however, contend that the program, along with other zero-rating programs, violates net neutrality provisions and fails to provide users with proper data security. The Telecommunications Law empowers IFETEL to develop rules on net neutrality and traffic management, which it is expected to do in the upcoming year.

Digital Activism

While online journalists and bloggers still face serious threats, such as cyberattacks, harassment, and physical violence, social media has continued to serve as an important forum for internet users in Mexico. In an act of everyday activism and in the face of significant risk, users make regular use of social media to provide critical warnings to local communities about dangerous cartel-related situations and to protest instances of corruption and violence by authorities and cartels.

In 2014, Twitter users launched the hashtag #TodosSomosAyotzinapa to organize protests against the kidnapping and murder of 43 students from a teaching college in Ayotzinapa, Guerrero on September 26, 2014. Frustrated with the lack of results in the investigation and the security situation in the country, with state government officials often implicated in violence, Mexicans took to the streets for over a month in a series of protests in the wake of the mass killing.

Social media in Mexico has also been used also as a tool for organizing to defend equal access to technology and freedom of expression online. In 2013, for example, a coalition of NGOs working on the project Internet Para Todos (Internet for All) turned to the internet to gather signatures for a petition to lobby the government to recognize internet access as a fundamental right. Due in large part

---

65 Internet.org changed its name to Free Basics in September 2015.
to the success of the coalition, Congress included internet access as a civil right in its 2013 reform of the Mexican Constitution.72

Activism based around social media also succeeded in forcing the government to amend several articles in a draft version of the Telecommunications Law before it was passed in 2014. In April 2014, activists and civil society organizations initiated an online campaign for revisions in the Telecommunications Law73 and succeeded in forcing the government to remove Article 197 of the draft law, which would have allowed authorities to temporarily block signals at “critical places and events” for the sake of national security, and Article 145, which would have allowed content to be blocked at the request of a user or on the order of an authority.74

**Violations of User Rights**

In 2014 and early 2015, Mexico continued to be one of the most hostile environments in the world for online journalists and bloggers, who were subjected to retaliatory violence from drug cartels, organized crime, and public officials, resulting in at least one murder of an online journalist between June 2014 and May 2015, out of eight murders of journalists in the same period. The Mexican government has used the poor security situation in the country as an excuse to dramatically increase surveillance. Evidence continued to emerge that the Mexican government engages in extensive surveillance of its citizens, and the new Telecommunications Law allows the Mexican government to request metadata from telecommunications companies and ISPs without a warrant.

**Legal Environment**

Despite legislation intended to increase the security of journalists and human rights defenders, the government has had little success in deterring attacks on journalists, bloggers, and activists, which are rarely punished in a country that ranks near the top in global surveys on impunity.75 While the upper echelons of the judiciary are viewed as independent, state-level legal bodies have frequently been accused of ineffectual conduct, biased behavior, and even harassment of online journalists. New legislation on surveillance jeopardizes user rights by allowing significant breaches of privacy and significantly increasing the potential for abuse in government surveillance.

The Mexican Constitution guarantees freedom of speech, freedom of the press, and privacy of personal communications. In mid-2013, the parliament passed a law to create a constitutional amendment regarding telecommunications, and a Constitutional Reform Decree was subsequently enacted by the Mexican president on June 10, 2013. Besides granting the government expanded powers to curtail monopolies in the telecommunications sector, the amendment established internet access as a human right and guaranteed net neutrality. Nevertheless, the Telecommunications Law, created as

Mexico

secondary legislation to the constitutional amendment and approved in July 2014, contains several provisions that pose a risk to privacy, including provisions that force telecommunication companies to retain data for two years, provide real-time geolocation data to the police, and allow security agents to obtain metadata from private communications without a court order (see Surveillance, Privacy, and Anonymity).

Although defamation was decriminalized at the national level in 2007, criminal defamation statutes continue to exist in some of Mexico’s 32 states.76 The penal code in Tabasco, for example, establishes penalties ranging from six months to three years of prison for those accused and sentenced for libel. Over the past year, however, some halting progress has been made in decriminalizing defamation. Carmen Olsen, a reporter from Baja California who was sentenced to two years on probation for libel, was finally exonerated after the local congress passed a law decriminalizing libel and slander.77 In July 2015, the governor of Tlaxcala sent an initiative that would decriminalize defamation to the state congress for consideration.78

In June 2012, the Law for the Protection of Human Rights Defenders and Journalists was passed in Mexico, establishing the Governmental Mechanism of Protection, an institutional body of government officials and civil society members charged with providing protection for threatened human rights workers and journalists.79 Among the law’s provisions is a requirement that state governments work in conjunction with federal authorities to ensure that protection is effectively extended to those under threat; as of March 2014, 31 of Mexico’s 32 states had signed agreements to this effect.80 While the legislation is promising in that it establishes a legal basis for protection and suggests an end to impunity for attackers, to date, capacity to implement the law has been lacking. In April 2014, the Governmental Mechanism came under criticism due to delays in processing approximately 57 percent of the 152 time-sensitive requests for protection.81

Prosecutions and Detentions for Online Activities

There were no documented cases of individuals detained, prosecuted, or sanctioned by law enforcement agencies on charges related to disseminating or accessing information on the internet. However, there is substantial suspicion that the arrest of the Mayan journalist Pedro Canché was at least partially in retaliation for a video and photos he posted on social media, which criticized the state government of Quintana Roo and showed an indigenous protest against increases in the price of water.82

---

Mexico

Canché was arrested on August 20, 2014 on charges of sabotaging the water supply after he was seen conducting interviews and filming at protests against the Drinking Water and Sewage Commission. He spent nine months in jail until he was set free on May 28, 2015, following a judge’s ruling in February that his detention was arbitrary and that he had been denied due process.\(^3\) Reporters Without Borders and Amnesty have criticized the detention, alleging that Canché was targeted for his work as a journalist.\(^4\)

Online reporters may also risk harassment and arrest when covering demonstrations and reporting on police action. On January 7, 2015, riot police arrested César Hernández Paredes and Gustavo Aguado, two editors of the online publication Revolución 3.0, when the journalists used their cell phone cameras to film the officers arresting two young men during a demonstration in Mexico City.\(^5\)

The officers took the cell phone of one of the editors, and then violently forced them into a police van. Several officers took photos of the editors in the van before releasing them.\(^6\)

**Surveillance, Privacy, and Anonymity**

Despite a constitutional requirement that any interception of personal communications be accompanied by a judicial warrant,\(^7\) the Mexican government has broad powers to track and surveil citizens. New legislation allowing authorities to access metadata without a warrant may jeopardize users’ privacy. Anonymity, on the other hand, is largely protected. After a 2008 requirement that cell phone users register with the government was revoked in 2012, there are no longer any official provisions regarding anonymity.

The Telecommunications Law, passed in July 2014, contains provisions that may threaten privacy. Article 189 of the law forces telecommunication companies to provide users’ geolocation data to police, military, or intelligence agencies in real time, and without a court order. Article 190 similarly forces providers to grant security agencies access to metadata at any time without a court order.\(^8\)

These provisions have received strong opposition from groups advocating for digital privacy and internet freedom.\(^9\)

The law further mandates that ISPs and mobile providers keep detailed records of users’ communications for two years. For the first year, ISPs and mobile providers must save the relevant data in a system that allows the competent authorities to consult the data electronically in real-time without a court order, or what some have worried amounts to “back-door access.” For the following year, the data must be stored in such a way that telecommunications companies can retrieve the data within

---


\(^8\) Artículo 189-190 de Ley Federal de Telecomunicaciones y Radiodifusión.

48 hours of being notified by authorities.\footnote{Artículo 189-190 de Ley Federal de Telecomunicaciones y Radiodifusión.} One of the major concerns raised by civil society groups is the vague language in the law, which allows for data requests by the “appropriate authority” but does little to establish parameters for who this authority might be. Corruption and weak rule of law among state governments—including the infiltration of law enforcement agencies by organized crime—also leave room for abuse to allow private communications fall into the wrong hands.

The Telecommunications Law expands on and partially replaces previous legislation that increased surveillance and allowed for real-time geolocation. In 2012, Congress passed a bill, known as the “Geolocation Law,” which amended existing legislation to allow the Federal Prosecutor (PGR) to obtain the real-time location of a mobile device for a limited list of criminal investigations (for example, kidnapping, extortion, or organized crime). At the time, critics warned about privacy concerns and the potential for abuse in warrantless surveillance,\footnote{Cyrus Farivar, “Mexican “Geolocalization Law” draws ire of privacy activists,” ArsTechnica, April 24, 2012, \url{http://bit.ly/1LY23cA}.} and the National Human Rights Commission brought a legal challenge before the Supreme Court. In January 2014, however, the Supreme Court upheld the law.\footnote{Luis Fernando, “Qué decidió finalmente la Corte sobre la geolocalización de celulares,” [What did the Court finally decide about the geolocation of cell phones] Nexos, February 2, 2014, \url{http://bit.ly/1OS1iZV}.} Of the two laws that were amended by the Geolocation Law, one was replaced by the 2014 Telecommunications Law, while the other (the Federal Code on Criminal Procedure), is set to expire in 2016 once it is replaced by the National Code on Criminal Procedure. Nevertheless, authorities’ powers of surveillance have only increased under the updated legislation. Under the 2014 Telecommunications Law, for example, geolocation is no longer restricted only to the Federal Prosecutor but is open to undefined “authorities,” nor is its use restricted to a limited number of prescribed cases.

Recent reports concerning a vast state surveillance apparatus further call into question the adequacy of privacy protections. In July 2015, a hack that resulted in a leak of internal documents from the surveillance company Hacking Team revealed that Mexico was the company’s biggest client worldwide and that the company had signed more than 14 contracts with various state and federal agencies. Civil society organizations have argued that these contracts are illegal because many of the agencies involved in the contract lack constitutional or legal authority to conduct surveillance or espionage.\footnote{The hack against Hacking Team occurred outside of the coverage period for this year. For more information about the revelations of Hacking Team’s operations in Mexico see Julio Sánchez Onofre, “Vulneración a Hacking Team confirma abuso de espionaje en México,” [Breach of Hacking Team confirms abuse of espionage in Mexico] El Economista, July 6, 2015, \url{http://bit.ly/1JBD07A}, see also Daniel Hernandez and Gabriela Gorbea, “Mexico is Hacking Team’s Biggest Paying Client -- By Far,” Vice News, July 7, 2015, \url{http://bit.ly/1WGbpmO}.} The media outlet Animal Politico has also accused the state government of Puebla of using Hacking Team exploits to target the political opposition and journalists, based on the fact that several leaked emails show that the company produced exploits that had subject lines or attachments directly addressed to opposition figures.\footnote{Ernesto Aroche, “El gobierno de Puebla usó el software de Hacking Team para espionaje político,” Animal Politico, July 22, 2015, \url{http://bit.ly/1T007rh}.}

The leaked information from Hacking Team is only the latest in a series of scandals involving Mexico’s surveillance apparatus. In July 2012, military sources leaked evidence, which was later confirmed by the Mexican army, pertaining to the Mexican army’s secret purchase of more than MXN 4 billion (more than US $300 million) of spyware engineered to intercept online and mobile phone communications.\footnote{Ryan Gallagher, “Mexico Turns to Surveillance Technology to Fight Drug War,” Future Tense (blog), Slate, August 3, 2012, \url{http://bit.ly/1T007rh}.} In addition to recording conversations and gathering text messages, email, internet naviga-
tion history, contact lists, and background sound, the surveillance software is also capable of activating the microphone on a user’s cell phone in order to eavesdrop on the surrounding environment. In 2013, reports also surfaced that FinFisher software is being used for surveillance in Mexico. Although a group of human rights organizations has called for a federal investigation into the use of espionage and intelligence tools, the government has yet to conduct or submit to any such investigation.96

The United States government has allegedly played a key role in funding and supporting the expansion of Mexico’s surveillance apparatus,97 for example through the installment of specialized surveillance equipment in 2006.98 This equipment, which comprises Mexico’s Technical Surveillance System, allows the government to “intercept, analyze and use intercepted information from all types of communication systems operating in Mexico.”99 Experts interviewed by NextGov.com in 2012 alleged that secret surveillance of private citizens is widespread in Mexico.100

Government requests to social media companies for information regarding users have increased significantly over the past year. Between January and December 2014, Facebook received 430 requests from the Mexican government for information related to 679 users, an increase of more than 100 percent compared to 2013. In 56 percent of the cases, Facebook released some information.101 Facebook did not reveal the type of information requested by the government, however. Between January and June 2014, Google received 111 requests from the Mexican government for user data of 144 users/accounts, an increase of 37 percent from the previous period. The company produced information in 79 of such cases.102

Intimidation and Violence

Violence against ICT users has continued to escalate in Mexico in recent years. In 2014, Reporters Without Borders listed Mexico as among the most dangerous countries in the world for media personnel.103 Threats and violence from drug cartels—and occasionally members of local government—have continued to plague online reporters. Between June 2014 and May 2015, eight journalists were murdered. At least one of these journalists worked exclusively online to report crimes, while another journalist who published both online and offline may have been murdered over information he posted on Facebook. Since the end of the coverage period, the situation has only worsened, with an additional four journalists murdered in July and August alone.

Maria del Rosario Fuentes Rubio, an administrator of Valor por Tamaulipas, a Twitter and Facebook

---

99 Beckusen, “U.S. Looks to Re-Up its Mexican Surveillance System.”
network reporting drug violence in the border state of Tamaulipas, was brutally murdered in Reynosa City, after being kidnapped on October 16, 2014. Fuentes Rubio was known for tweeting danger alerts about drug cartel violence and urging people to report violent incidents to the police. Her attackers used her own mobile phone and Twitter account to post gruesome photos of her assassination.104 The year before her murder, Valor por Tamaulipas had temporarily shut down after a cartel circulated pamphlets offering a MXN 600,000 reward (approximately US$36,764) for information about the network administrators.105

On January 24, 2015, authorities found the decapitated body of José Moisés Sánchez Cerezo, an online and print journalist who was kidnapped from his home in Medellín de Bravo earlier in the month. Sánchez founded and operated La Unión, a small print and online newspaper, although he had not published a print or online edition for several months before his murder, due to financial constraints. In the lead-up to his murder, Sánchez was active on Facebook, posting critical commentaries and links, including links to articles about shortcomings in local law enforcement and photographs of a protest against the governor, Javier Duarte de Ochoa. The Veracruz state attorney implicated Omar Cruz Reyes, the mayor of Medellín, as a suspect in the killing, although no formal charges have been pressed.106

Killings continued after the end of the coverage period of this report. On July 2, 2015, authorities found the body of Juan Mendoza Delgado, the director and founder of the local news website Escribiendo la Verdad (which translates to “Writing the Truth”). Although authorities claimed that Mendoza had been run over by a car, human rights organizations are investigating to see whether Mendoza’s death was related to his writing, which was often highly critical of local politicians and organized crime.107 On August 3, 2015, photojournalist Rubén Espinosa was found dead in Mexico City after fleeing his home state of Veracruz where he had been threatened for his journalistic work. Espinosa worked for local and national news organizations, as well as the online photo agency Cuartoscuro.108

Although threats, verbal attacks, and physical attacks that do not lead to death are less likely to make the news, these aggressions are pervasive. On January 14, 2015, for example, Yohali Resendiz, a journalist working for Grupo Imagen, reported receiving threats—including death threats and videos of violent attacks on women—via Twitter after she reported on arbitrary arrests of children in Mexico City.109 Such aggression can contribute to self-censorship and have an enormous toll on journalists and activists, forcing some of them to flee their homes or professions out of fear of violence.

Technical Attacks

There were at least six major cyberattacks against online news organizations and human rights groups’ websites between June 2014 and May 2015:

Mexico

- Juan Carlos Solis, a journalist in Chihuahua, reported that his Facebook account was hacked on June 28, 2014 for several days. The attackers posted pornographic photos and videos on his account, as well messages of support for political parties. Solis said that all information criticizing the state government and showing arbitrary arrests of human rights defenders was erased from his Facebook account.110

- *Diario Cambio*, a media organization based in Puebla, reported that it was subject to a cyberattack on July 30, 2014, after running a story that suggested that rubber bullets fired by state police were the cause of death of a boy who was killed during a confrontation between state police and protesters in Chalchihuapan.111

- The news portal *Sin Embargo* was attacked on November 11, 2014 with a DDoS attack that shut down the website for several hours.112 Editors reported that the cyberattack took place after the website posted photos of a local Mexico City major wearing military uniform, close to military vehicles.113

- On November 18, 2014, e-Consulta, an online news organization based in Puebla, reported that a hacker or a group of hackers erased comments, stories, photos, and editorial columns from its site.114 Sources told the e-Consulta editors that Mexico City-based hackers, presumably hired by the Puebla state government, were responsible for the attack. The version could not be corroborated.115 The digital newspaper’s editor, reporters, and managers have been under a campaign of arrests, defamation lawsuits, and kidnappings since 2012, including an attack in July 2013, when a burglar broke into e-Consulta’s Puebla office and stole the computers of the general director and the managing director.116

- Three websites of the Mexican chapter of Article 19, an international nonprofit organization focused on freedom of expression, were attacked over the course of three days via a Cross-Site Scripting (XXS) attack, a type of cyberattack that allows attackers to inject script into publically viewed webpages, on February 5, 2015.117 The attacks affected accessibility to Article 19 websites focused on the security of journalists.

- On April 18, 2015 the Aristegui Noticias website suffered a DDoS attack that shut down the publication for four days. Days before, the news website had run a story about the involvement of federal police officers in a massacre of civilians in Michoacan.118

---

Mexico

Technical attacks are now a central tactic in governmental and non-state actor attempts to suppress freedom of expression, and entities that commit cyberattacks do so with relative impunity. Recently, online news outlets have started to protect themselves against DDoS attacks by contacting Deflect, a Canadian nonprofit organization protecting websites of human rights organizations and independent media publications.119

Key Developments: June 2014 – May 2015

- Unlike last year, there were no instances of blocking reported over the coverage period. Independent news site Lakome is back online after journalist Ali Anouzla was released from prison, although the terrorism-related charges for his media reporting have not been dropped and continue to pose a significant chilling effect on investigative reporting (see Blocking and Filtering and Media, Diversity, and Content Manipulation).

- Authorities proposed changes to the press code that would remove jail sentences for journalistic crimes, except in cases when journalists fail to pay a fine—which remained steep relative to the limited operational budgets of most news outlets. The proposed draft also mandates the registration of online journalists in a move that may bring them further under the control of the government, stifling free reporting (see Legal Environment).

- Seventeen-year-old rapper Othman Atiq, known as Mr. Crazy, was jailed from August to November 2014 under charges of “insulting a state institution,” “incitement to consume drugs,” and producing material “harmful to public morality.” Atiq’s music videos—some of which feature more than a million views on YouTube—depict the troubled lives of unemployed youth in Casablanca and were used as evidence in his trial (see Prosecutions and Arrests for Online Activities).

- News websites Badil and Goud were taken to court for allegedly defaming public officials. Hamid El Mehdaoui, Badil editor-in-chief, was given a four-month suspended sentence and a fine in June 2015 for an article investigating the death of an activist while in police custody. That same month, the news site Goud was ordered to pay MAD 500,000 (US$51,000) for an article that accused the king’s private secretary of corruption. The steep fine may bankrupt the independent news site (see Prosecutions and Arrests for Online Activities).
Morocco

Introduction

Internet freedom has stagnated during the coverage period. Several news sites were targeted for investigative pieces that allegedly defamed public officials, while a seventeen-year-old rapper was jailed for his music videos uploaded to YouTube. These moves follow last year’s prosecution of Ali Anouzla, an influential investigative reporter and editor-in-chief of Lakome.com. Although Anouzla has since been released pending trial, his arrest and the blocking of his news site has had a notable chilling effect on Morocco’s digital landscape. Many sites had looked to Lakome for maintaining a high ceiling of free expression in the country, particularly in its coverage of the monarchy. Instead, the outlandish charges of “advocacy of acts amounting to terrorism offenses” and “providing assistance to perpetrators or accomplices of acts of terrorism” directed at a credible journalist demonstrated the extent to which the state is prepared to silence dissent. While authorities may show a permissive attitude to social media and user-generated content, journalists and civil society actors still take care not to cross red lines in order to avoid legal threats, trumped up charges, and the hacking of personal accounts.

Social media has triggered a revival of the media’s traditional watchdog function, acting as a check on the misconduct of the political regime. It has also been used as a tool for nascent political movements to organize and mobilize supporters across the country, particularly in the context of the Arab Spring. The February 20th Movement, which started on Facebook and relies heavily on digital media for communication, has held rallies throughout the country demanding democratic reforms, a parliamentary monarchy, social justice, greater economic opportunities, and more effective anticorruption measures. Two weeks after the first demonstrations, King Mohamed VI responded by announcing new constitutional reforms in which he promised to devolve limited aspects of his wide-ranging powers to an elected head of government and the parliament. Included in this reform package were provisions to grant greater independence to the judiciary and an expansion of civil liberties. The king’s proposals were approved by 98.5 percent of Moroccan voters in a popular referendum held on July 1, 2011, in which voter turnout was 84 percent. These measures resulted in a lifting of all politically-motivated filtering.

The emergence of trusted online news publications staffed with professional online journalists has threatened the authorities’ control over the country’s media sphere. While digital media remains more diverse than television and newspapers, recent events indicate the authorities are keen to clamp down. A new “digital code” (code numérique) and press code have been drafted by government ministries in a bid to introduce greater regulations and restrictions. Through the allocation of advertisements, directives about what can be reported, progovernment trolls, and court cases against journalists, the state ensures that controversial issues in the country are left untouched and leading newsmakers willingly self-censor. This situation is reinforced by the state’s use of surveillance technology to further strengthen the atmosphere of fear among online journalists and activists.

---

1 Interview with Ali Anouzla a journalist, conducted on June 27, 2014.
2 Interview with Aboubakr Jamai, a Moroccan journalist, founder of progressive magazines such as Le Journal Hebdomadaire and Assahifa al-Ousbouija; 2003 recipient of International Press Freedom Award, conducted on January 8 2014.
Morocco

Obstacles to Access

Access continues to increase in Morocco, with the majority now using mobile phones to browse the internet. A digital divide between Morocco's urban and rural areas and a low adult literacy rate continue to marginalize some population groups online. However, lower prices, a growing liberalization of the ICT sector, and fairer regulations signal positive trends when it comes to the government's goal of providing universal access.

Availability and Ease of Access

Internet access in Morocco has increased steadily in recent years, although obstacles remain in place in certain areas of the country. The internet penetration rate grew from 41.3 percent in 2009 to 56.8 percent in 2014, according to the International Telecommunication Union (ITU).\(^3\) By end of 2014, just shy of 3 in every 100 inhabitants possessed a fixed-broad subscription. Mobile penetration reached 133 percent. According to Morocco's regulator, 30 percent of users have an internet subscription, of which some 90 percent were 3G mobile internet subscribers. Mobile internet subscriptions increased by almost 82 percent over the calendar year.\(^4\)

Internet access is currently limited to educated and urban segments of Morocco's population. There is a major discrepancy in terms of network coverage between urban and rural areas. Telecommunications companies do not abide by the ITU principle of telecommunications as a public service, instead preferring to invest in more lucrative urban areas. Rural inhabitants constitute 39.7 percent of the overall population\(^5\) and while many have access to electricity, television, and radio, most do not have access to phone lines and high speed internet. The high rate of illiteracy is another obstacle (43 percent of Moroccans aged 10 and above are illiterate). The ITU's ICT Development Index (IDI) ranks Morocco 89th, primarily due to a low adult literacy rate, low gross secondary enrollment ratio, and low gross tertiary enrollment ration.\(^6\)

Research universities led the development of the internet in Morocco from the early 1990s, with internet access extended to the general public in 1996. Initially, the internet’s diffusion was slow in Morocco due primarily to the high cost of computers and poor infrastructure.\(^7\) Under the combined impact of the liberalization, deregulation, and privatization of the telecommunications sector, as well as the legal and technological modernization of Moroccan broadcasting media, a growing and dynamic digital media market has emerged.

The Moroccan government has undertaken several programs over the years aimed at improving the country's ICT sector. Most recently, the Note d'Orientations Générales 2014-2018\(^8\) (Guidelines for the Development of the Telecoms Sector 2014-2018) provides the framework for the development

---


6 Morocco is ranked 114th in the IDI Skills sub-index, which measures human capacity and the population’s abilities to use ICTs. See International Telecommunication Union, Measuring the Information Society.


8 ANRT, Rapport Annuel 2013.
Morocco

of ICTs in the next four years. The program aims to provide fiber-optic and other high speed connections throughout the country, to reinforce the existing regulatory framework, and to provide universal access.

As a result of previous government efforts, internet use remains relatively affordable. For a 3G pre-paid connection of up to 7.2 Mbps, customers pay MAD 223 (US$26) for initial connectivity fees and then MAD 10 per day (US$0.82) or MAD 200 per month (US$23.6). Internet users pay on average MAD 3 (US$0.35) for one hour of connection in cybercafes.

Restrictions on Connectivity

Authorities did not impose large scale restrictions on connectivity over the past year. However, the centralization of Morocco’s internet backbone facilitates the potential control of content and surveillance. In terms of terrestrial regional connectivity, Maroc Telecom owns and controls a fiber-optic backbone of more than 10,000 kilometers (km) covering the whole territory. The national railroad company, Office Nationale des Chemins de Fer (ONCF), and the national electricity and water utility, Office National de l’Electricité et de l’Eau Potable (ONEE), have also built 2000 km and 4000 km fiber-optic infrastructures, respectively. The state owns 30 percent of the shares of Maroc Telecom and controls the railway as well as electricity and water companies, hence giving it access to the entire regional internet backbone.

Morocco’s national and international connectivity has a combined capacity exceeding 10 terabits per second (Tbps). The three telecom operators (Maroc Telecom, Medi Telecom, and INWI) have access to international connectivity with Maroc Telecom controlling three submarine stations, Méditel (with redundant connectivity) controlling more than two submarine cables and stations, and INWI controlling one cable.

ICT Market

Maroc Telecom, Medi Telecom, and INWI are the three internet service providers (ISPs) and mobile phone companies in Morocco. Maroc Telecom (Ittissalat Al Maghrib, IAM) is a former state company that held a monopoly over the telecoms sector until 1999. That year, the National Agency for the Regulation of Telecommunications (ANRT) granted licenses for Medi Telecom and INWI. Medi Telecom is a private consortium led by Spain’s Telefónica, while INWI (formerly WANA, Maroc Connect) is a subsidiary of Ominum North Africa (ONA), the leading Moroccan industrial conglomerate also owned by the royal family. All three companies have submitted applications for 4G mobile phone licenses, following a call for tenders from the ANRT.

---

10 Gelvanovska, Rogy, and Rossotto, Broadband Networks in the Middle East and North Africa: Accelerating High-Speed Internet Access.
Regulatory Bodies

Service providers such as ISPs, cybercafes, and mobile phone companies do not face any major legal, regulatory, or economic obstacles. The ANRT is a government body created in 1998 to regulate and liberalize the telecommunications sector. Its board of directors is made up of government ministers and its head is appointed by the king. The founding law of the ANRT extols the telecommunications sector as a driving force for Morocco's social and economic development, and the agency is meant to create an efficient and transparent regulatory framework that favors competition among operators. A liberalization of the telecoms sector aims to achieve the long-term goals of increasing GDP, creating jobs, supporting the private sector, and encouraging internet-based businesses, among others. While Maroc Telecom, the oldest telecoms provider, effectively controls the telephone cable infrastructure, the ANRT is tasked with settling the prices at which the company's rivals (such as Medi-Telecom and INWI) can access those cables. Thus the ANRT makes sure competition in the telecoms market is fair and leads to affordable services for Moroccan consumers.

Some journalists argue that the ANRT is a politicized body lacking independence, citing the fact that its director and administrative board are appointed by a Dahir (Royal Decree). However, international organizations such as the World Bank and the ITU have not expressed any major criticism about the ANRT's neutrality.

The allocation of digital resources, such as domain names or IP addresses, is carried out by organizations in a non-discriminatory manner. According to the Network Information Centre, which manages the ".ma" domain, there were 57,492 registered Moroccan domain names in April 2015.

Limits on Content

After last year’s dramatic blocking of Lakome, this coverage period witnessed the restoration of the news website. However, since one of its editors-in-chief continues to await trial on terrorism charges, the move has created a lasting chilling effect on Morocco's digital landscape. Although authorities do not block or filter online content, the general atmosphere of fear has increased self-censorship. This is particularly marked among professional journalists working in well established online news organizations, who remain the primary target of the authorities' backlash.

Blocking and Filtering

The government did not block or filter any websites over the coverage period. The last instance of government blocking of online content dates back to October 2013 when the Attorney General ordered the ANRT to block the Arabic- and French-language websites of the investigative news site.

13 Interviews with Dr. Hamid Harroud and Dr. Tajjedine Rachdi, director and former director of Information Technologies services of Al Akhawayn University in Ifrane, conducted on March 20 and 22, 2015.
17 Network Information Centre, the service that manages the domain .ma, is owned by Maroc Telecom. There are calls for domain.ma to be managed by an independent entity, not a commercial telecoms company.
18 This service is owned by Maroc Telecom. Network Information Centre, accessed 31 March 2015, http://www.registre.ma/?page_id=73.
Morocco

*Lakome*. Its Arabic-language editor in chief, Ali Anouzla, was arrested one month earlier for citing an article in the Spanish newspaper *El País*, which contained an embedded YouTube video attributed to Al Qaeda in the Islamic Maghreb (AQIM). Activists and observers believe *Lakome* was blocked for its critical stance towards the monarchy.

Both the Arabic and the French versions of the site had published an investigative report on the exploitation of sand pits showing the extent of corruption and the culture of impunity deeply rooted in the highest level of the regime. The sites were also the first to announce the scandal surrounding the royal pardon granted to the convicted pedophile Daniel Galván Viña on July 31, 2013. This event garnered significant international media coverage from satellite television stations such as BBC, CNN, France24, Al Jazeera and others, all of whom relied heavily on *Lakome* for their information. As a result, the site achieved international fame and notoriety with the local authorities. Indeed, local bloggers and activists observed that *Lakome* had become a liability to the Moroccan regime, with its editorial independence, investigative stories, and relentless refusal to self-censor. Zineb Belmkaddem, a blogger and activist, noted the site’s “readership, as well as its impact, were growing” and cited the blocking of *Lakome* as an example of what happens when journalists do not acquiesce to calls (and even threats) to soften their tone when reporting on government affairs.

Social media and communication services such as YouTube, Facebook, or Twitter and international blog-hosting services are available in the country. Websites are available which discuss controversial views or minority causes, such as the disputed territory of Western Sahara, the Amazigh minority, or Islamist groups. Despite numerous reports to the contrary, Google Earth was found to be accessible in tests conducted by Freedom House in several cities and on a range of different devices. The service had been reportedly blocked in August 2009.

Similarly there are no restrictions on anonymous proxy tools and Voice over Internet Protocol (VoIP) services. However, in February 2012 there was a report that Maroc Telecom briefly disrupted VoIP services such as Skype, TeamSpeak, and Viber in order to tamper with the quality of the calls. Some speculated that the actions were motivated by financial concerns over competition to traditional fixed-line services provided by the telecommunications company.

**Content Removal**

While the government does not block online content, it maintains control over the information landscape through a series of restrictive laws that can require the shutting down of publications and removal of online content. Under the 2002 Press Law, the government has the right to shut down any publication “prejudicial to Islam, the monarchy, territorial integrity, or public order,” and it maintains prison sentences and heavy fines for the publication of offensive content (see “Legal Environment”).

---


20 Interview with Zineb Belmkaddem, a Moroccan blogger, citizen journalist, and 20th February activist, conducted on January 15, 2014.


Morocco

The antiterrorism law\(^\text{23}\) gives the government sweeping legal powers to filter and delete content that is deemed to “disrupt public order by intimidation, force, violence, fear or terror.”\(^\text{24}\) Article 218-6 assigns legal liability to the author and anybody who in any way helps the author to disseminate the apology for acts of terrorism, a provision which would include site owners and ISPs. Intermediaries must block or delete infringing content when made aware of it or upon receipt of a court order.\(^\text{25}\)

While the law was ostensibly designed to combat terrorism, the authorities retain the right to define vague terms such as “national security” and “public order” as they please, thus opening the door for abuse. Many opposition news websites, such as *Lakome* and *Febrayer* are hosted on servers outside of the country to avoid being shut down by the authorities.

The government also resorts to more ad hoc, extralegal means to remove content deemed controversial or undesirable. For example, *Hespress*, which in the past featured content both supportive and critical of the government, has deleted videos of street protests and interviews with opposition figures from the site out of fear or pressure from authorities.\(^\text{26}\)

**Media, Diversity, and Content Manipulation**

Owing to self-censorship on key political topics, the Moroccan online media landscape lacks in diversity and investigative journalism. Online news outlets receive unofficial directives not to report on controversial issues, or not to allow certain voices to be heard. In a state that punishes investigative reporting and whistleblowing, people with sensitive information tend to stay quiet to avoid possible retribution. Debates on issues related to the monarchy do not make news, both in traditional and online media. For example, the release of Prince Hicham’s “explosive”\(^\text{27}\) book, *Journal d’un Prince Banni* [Diary of a Banished Prince] in April 2014\(^\text{28}\) surprisingly did not trigger any discussion or reaction in the country, which many observers link to self-censorship and fear of reprisals.\(^\text{29}\)

The existing atmosphere of fear among journalists online was strengthened with the arrest of Anouzla and the ensuing blocking of *Lakome*.\(^\text{30}\) Given Anouzla’s reputation for independence, nonviolence, and pushing boundaries, many saw the charges of “advocacy of acts amounting to terrorism offenses” and “providing assistance to perpetrators or accomplices of acts of terrorism” as a clear at-

---

\(^{23}\) The Anti-Terrorism law, passed in 2003 after the 2003 terrorist attacks in Casablanca. On 16 May 2003, Morocco was subject to the deadliest terrorist attacks in the country’s history. Five explosions occurred within thirty minutes of each other, killing 43 people and injuring more than 100 in suicide bomb attacks in Morocco’s largest city, Casablanca. Morocco has been a staunch ally of the U.S. The 14 suicide bombers all originated from a poor suburban neighborhood in the outskirts of Casablanca.


\(^{26}\) Interviews with Driss Ksikess, a well-known journalist and former editor in chief of Nichane and Reda Benotmane, a prominent activist and founding member of Freedom Now, conducted on April 2-3 2015.


\(^{28}\) First cousin of King Mohammed VI and third in the line of succession to the throne, Prince Moulay Hicham gained the nickname “Red Prince” because of his pro-democracy positions and his calls for reforms of the monarchy. The book is an account of a member of the royal family who expressed his views on the political system in Morocco, and called for the reform of the Mekhzen and the institution of the monarchy.

\(^{29}\) Interviews with digital activists and online journalists.

\(^{30}\) Interviews with Aboubakr Jamai, Hisham Almiraa, Zineb Belmkaddem, IbnKafka, Driss Ksikess, Reda Benotman, and two other interviews conducted with online activists who want to remain anonymous from February 2013 and April 2015. Hereafter, interviews with digital activists and online journalists.
Morocco
tempt to silence a dissenting voice.\textsuperscript{31} Many online and offline news outlets looked up to \textit{Lakome} for maintaining a high ceiling for freedom of expression, especially in matters related to the monarchy, wherein most political power is concentrated.\textsuperscript{32}

Compounding self-censorship and fear are the personal attacks and derogatory comments received by activists and opinion makers online for openly criticizing government policies.\textsuperscript{33} Numerous accounts are created on Twitter and Facebook with the sole purpose of harassing, intimidating, and threatening activists. Activists believe that these progovernment commentators are also equipped with direct or indirect access to surveillance tools, since they have often obtained private and personal information on other users.\textsuperscript{34} There is no clear indication regarding the identity behind the accounts and whether they are state-sponsored or simply overzealous private individuals. However, due to the amount of time and energy needed to engage in such activity, and the access they have to private information, there are serious doubts that these are private citizens acting on the basis of their own personal resolve.

The government also uses financial pressure to push the most outspoken print media publications into closure or bankruptcy. Advertising revenue provided by the government or government-linked companies is not split fairly between independent and progovernment publications.\textsuperscript{35} In addition to state-run and opposition news outlets, the Moroccan media contains a variety of “shadow publications,” nominally independent but editorially supportive of the state.\textsuperscript{36} The news outlets exist primarily to divert airtime from more serious and engaging news portals and to compete over online advertising money and audience share. There is no evidence to link these publications to a larger state strategy to counter the growth of voices of dissent. However, it is important to note that these shadow publications receive large amounts of advertising, possibly in return for their progovernment bias. Powerful business entities, such as the three telecommunication companies, are known to adhere to state pressure to withdraw advertising money from news outlets that run counter to the state-owned media narrative.\textsuperscript{37} In a recent example of this, the Office Chérifien des Phosphates (OCP) and Caisse de Dépôt et de Gestion (CDG),\textsuperscript{38} two state-owned companies that do not offer any particular products to Moroccan consumers, are now buying advertising time and space. This move is meant to obtain positive media coverage, avoid negative publicity, and secure media outlets for their press releases.

The state, however, does not limit the ability of online media to accept advertising or investment from foreign sources, which is crucial for maintaining a profitable business and ensuring that citizens can access a range of different opinions and news sources. In addition, webhosting and free blog-

\begin{itemize}
\item \textsuperscript{31} Interview with Aboubakr Jamai.
\item \textsuperscript{32} Interview with Ali Anouzla.
\item \textsuperscript{33} Interview with Ali Anouzla.
\item \textsuperscript{34} Interview with Zineb Belmkaddem.
\item \textsuperscript{35} Interview with Driss Ksikess.
\item \textsuperscript{36} Interview with Driss Ksikess.
\item \textsuperscript{37} According to \textit{The Report: Emerging Morocco 2013} by Oxford Business Group, Maroc Telecom, Medi Telecom, and WANA Corporate spent three times more the amount of the second sector in terms of advertising with 1.3 bn MAD (£115.6 M). In 2011, according to l’\textit{Economiste.ma}, telecommunications advertising spending represents 23% of the total advertising market share. See: “INVESTISSEMENTS PUBLICITAIRES LA TÉLÉ EN PERTE DE MARCHÉ,” \textit{L’ECONOMISTE}, November 30, 2011, accessed March 29, 2015, \url{http://bit.ly/1KxtrE9}.
\item \textsuperscript{38} The OCP is the world’s largest exporter of phosphate and its derivatives. The CDG is a state institution in charge of collecting and managing specific state funds and savings.
\end{itemize}
ging services are freely accessible. ISPs are not known to limit bandwidth availability to discriminate on the basis of content.

The most remarkable change in internet use among Moroccans continues to be the growing interest in social media and user-generated content, as well as domestic news portals. In 2010, the top ten most visited websites did not include any Moroccan news websites.39 By 2015, three online news portals made it to top 10 most visited site, with Hespress remaining as the most popular website in Morocco with estimated 600,000 unique visitors per day. It is ranked fourth after Google, Facebook, and YouTube. Besides Hespress, Alyaoum24, and Hibapress are now ranked seventh and ninth, respectively. The Moroccan classified ads site avito.ma, is ranked fifth and Moroccan sports site Elbotala is ranked 11th bypassing the pan-Arabic sports website Kooora which ranked top ten in previous years.40 Facebook users grew by 490 percent from 860,000 to more than 5.1 million between 2009 and 2015, and the social network is the most visited website in the country.41

Digital Activism

Internet users take advantage of various social media tools to educate, organize, and mobilize people around a wide variety of issues. One recent instance of online activism resulted in the sacking of Mohamed Ouzzine, the Minister of Youth and Sports. Morocco was host of the FIFA World Club finals in December 2014. The third game took place in the newly rebuilt stadium of the capital Rabat and due heavy rain, the pitch turned into a pool which created significant problems for the players of the Mexican club Cruz Azul and the Australian club Wanderers. Videos and commentary on the event were extensively shared on Facebook, YouTube, and Twitter. The videos mocking the event were also aired in many international TV stations. As in the previous instances of digital mobilization, Moroccan mainstream media including state controlled broadcasting could not ignore the event and they ended up reporting on it. As an outcome of these events, the King suspended the minister from his duties and later on officially dismissed him. It is not clear if the King’s decision was due to online pressure or if it was an isolated decision.

Twitter has also been used as a tool for whistleblowing. Since October 2014, the account @chriscoleman has been releasing hundreds of classified diplomatic documents from Morocco’s Ministry of Foreign Affairs.42 The account operates under the pseudonym “Le Makhzen,” a term used to designate the old form of government under the Alaouite dynasty which is still used to refer to the most traditional forms of governance in the country. The tweets consist of releasing documents such as confidential correspondences, money transfer orders, confidential emails, and other documents that cite members of the royal family, diplomats, members of civil society, and journalists. The documents accuse a number of French and American journalists of being corrupted by the Moroccan government to write favorable media coverage of the Western Sahara. The author of this campaign clearly aims at destabilizing the Moroccan regime and appears motivated by the Western Sahara conflict. According to journalist Jean-Marc Manach, co-founder of the Big Brother Awards,

---

40 Google, Facebook, YouTube, hespress, and Google Morocco were the five most visited sites in 2014. See, Alexa, “Top Sites in Morocco,” accessed March 31, 2015, http://www.alexa.com/topsites/countries/MA.
some of these documents are authentic while others are manipulated. Mbarka Bouaida, deputy minister of foreign affairs, stated that the tweets are motivated by pro-Polisario militants funded and supported by Algeria. Foreign Minister Salahdine Mezouar has launched an investigation into whether these classified government documents were willingly leaked or if it is a matter of hacking.\textsuperscript{43} Given the general atmosphere of self-censorship and fear among journalists, these leaks did not trigger a public debate and there were no consequences other than the internal investigation.

### Violations of User Rights

Moroccan laws on criminal defamation and antiterrorism continue to pose a threat to free speech. A new press code containing several positive elements was released for public consultation in October 2014. While the proposed law eliminates jail time for the press, it mandates the registration of online journalists in a move that could bring them further under the authorities’ control. Arrests and prosecutions of ordinary social media users remained rare, but authorities targeted well known activists, news staff, and even rappers in order to silence those with significant influence over the public.

### Legal Environment

The constitution contains provisions designed to protect freedom of expression, but there are shortcomings in their enforcement. The 2011 constitution, passed by referendum to curtail public protests at the onset of the Arab Spring, recognizes all Moroccan citizens as equals before the law and Article 25 guarantees all citizens “freedom of opinion and expression in all its forms.”\textsuperscript{44} Although the 2011 constitution strengthened the judiciary as a separate branch of government, the judicial system in Morocco is far from independent. The king chairs the High Council of Judicial Power and appoints its members. As such, the courts often fail to produce fair and balanced rulings, frequently basing their decisions on recommendations from security forces.\textsuperscript{45}

The constitution also guarantees freedom of information. Article 27 states that Moroccan citizens have the right to access information held by the government, elected institutions, and all public service institutions, except in cases in which doing so would violate national security, the privacy of individuals, or constitutional freedoms. For this constitutional right to become reality, a series of public policy debates are taking place to devise policies that would guarantee citizens access to information. However, given the authoritarian nature of the state, many activists are pessimistic and believe the end result will most likely lead to a stifling of internet freedom under the guise of privacy, national security, and counterterrorism. As of mid-2015, no new outcomes have been reached.

The gravest legal threat to internet freedom in Morocco remains laws that restrict the type of material that can be communicated online. Chief among these are the 2002 press code and the 2003 antiterrorism law that outline criminal penalties for any criticism of “sacred” issues such as the monarchy, Islam, and territorial integrity. Crucially, these laws continue to be applied to online activity, resulting in the prosecution of several users for content posted online. Article 218-2 of the antiterrorism law


also proscribes prison terms of 2 to 6 years and fines of MAD 10,000 to 200,000 for those convicted of apology for acts of terrorism, through offline as well as online speech.46

Numerous articles within the press code are problematic. Article 38 defines “incitement to commit a crime” as any provocative speech that was uttered, written, printed, sold, or distributed in public places, meetings, as well as any audiovisual and electronic media. Article 41 stipulates that anyone who offends the institution of the monarchy, king and the royal princes and princesses, Islam, and the territorial integrity will be imprisoned for three to five years and must pay a fine of MAD 10,000 to 100,000 (roughly US$800 to 8,000). The publication can be suspended for up to three months or can be permanently banned. Articles 45, 46, and 47 of the 2002 press code stipulate that defamation against the courts, the military, public administrations, members of the government, and any public person are punishable by a prison term of one month to one year. Similarly, Article 52 outlaw criticism of foreign heads of state, foreign ministers, and diplomatic envoys residing in Morocco by stipulating punishments of one month to one year imprisonment and a fine of MAD 10,000 to 100,000 (US$800 to $8,000). Judges often apply these vague and oppressive laws to the online domain.

In an attempt to modernize the press code, the minister of communication released an updated version for review and consultation by civil society in October 2014.47 The code eliminates jail sentences for journalists and establishes a self-regulatory body. However, Articles 34 and 35 stipulate that online news portals must register their domain names in Morocco to be able to obtain press cards and benefit from state support. News portals must also obtain three types of authorizations, valid for one year at a time: from the High Authority of Audiovisual Communication (HACA)48 to post online videos, from the Moroccan Cinema Center (CCM)49 to shoot film, and from the ANRT to host domain names under press.ma. These organizations are state-controlled and can easily be influenced to deny authorizations or reject renewals for political purposes. These measures will instill the culture of prior restraint and fortify self-censorship. In addition, while prison terms for journalists have been removed, guilty parties can be imprisoned if they fail to pay proscribed fines.50

For many activists, another indication that the regime plans to stifle internet freedom was the release of a draft law on the internet called the *Code Numérique* (digital code) in November 2013.51 The draft was prepared by the Ministry of Trade, Investment and Digital Economy and aimed to reinforce the legislative framework of digital communication in Morocco by addressing e-government, e-marketing, e-commerce, digital security, and trust.52 As such, some aspects of the law were promoted by activists as positive. However, several of the bill’s provisions threatened internet freedom. For instance, Article 73 prohibited content deemed to be immoral, against public order, violent or

---

48 The High Authority for Audiovisual Communication (Haut Autorité de la Communication Audiovisuelle, HACA) was created in 2002 and mandated to establish the legal framework for liberalizing the audiovisual sector, and to oversee a public service broadcasting (PSB) sector.
49 *Le Centre Cinématographique Marocain* (CCM) is in charge of the organization and promotion of the film industry in Morocco and it oversees the application of the legislative and regulation of the sector.
50 Interview with Reda Benotmane, a prominent activist and founding member of Freedom Now, conducted on April 2-3 2015.
inciting violence, as well as any expression seen to undermine Islam, public policy or the privacy of individuals. The proposal’s broad wording thus would have led to a significant increase in blocking of websites.53 In response, a group of activists set out to crowdfund a new version of the digital code, critiquing aspects of the existing bill.54 The minister of industry, commerce, investment and digital economy announced in a tweet that he withdrew the draft bill in December 2013, arguing that the digital code is so important that it necessitates broad consensus.55

**Prosecutions and Detentions for Online Activities**

Moroccans continue to face the possibility of unjust arrest and prosecution for their online activities, particularly for material that is seen as critical of state officials.

Seventeen-year-old rapper Othman Aïtq, known as Mr. Crazy, was jailed from August to November 2014 under charges of “insulting a state institution,” “incitement to consume drugs,” and producing material “harmful to public morality.” Aïtq’s music videos—some of which feature more than a million views on YouTube—depict the troubled lives of unemployed youth in Casablanca and were used as evidence in his trial.56

In June 2015, Hamid El Mehdouai, editor of the news website Badil, was convicted of criminal defamation and given a four-month suspended sentence by a Casablanca court for allegedly defaming the head of Morocco’s General Directorate of National Security, Abdellatif el Hammouchi.57 El Mehdouai had published an article about the death of Karim Lachaqr, an activist who died in police custody in May 2014. Both he and his source (not a journalist) were ordered to pay combined damages of MAD 100,000 (US$10,000) or face imprisonment.

That same month, a Casablanca court ordered the news site Goud to pay MAD 500,000 (US$52,000) for civil defamation charges. Goud was targeted for an article that accused the king’s private secretary, Mounir El-Majidi, of corruption. The steep fine may bankrupt the independent news site.58

Journalist Ali Anouzla, who was arrested in September 2013, continues to face charges of “advocacy of acts amounting to terrorism offenses” and “providing assistance to perpetrators or accomplices of acts of terrorism.” Anouzla is the editor-in-chief of the French-language version of Lakome, a news site, who targeted for an article he had written on jihadist threats to Morocco in which he provided a link to a Spanish site, which in turn had embedded a jihadist video. He was released on bail on October 25, 2013 and his trial has been continually postponed.59

53 “Will Morocco Regulate the Internet? An Interview with Zineb Belmkaddem and @IbnKafka.”
Morocco

Surveillance, Privacy, and Anonymity

Given the absence of blocking and filtering, Moroccan activists identified surveillance as the most dangerous instrument in the hands the regime. The awareness among activists that they are systematically monitored impacts the way activists perceive the risk they take and the margin of freedom that they have. Hisham Almiraat, the co-founder of the website Mamfakinch and one of the leaders of the February 20th Movement, explained that the state’s capacity to own and reconstruct one’s personal story, based on surveillance and monitoring, allows authorities to “assassinate your character and use your own information to hurt you.” According to Zineb Belmkaddem, “surveillance entails the stealing of data and data is private property... it’s like the state coming to my home every day to steal my belongings.” Reports and interviews have revealed the use of malware products from Italian company Hacking Team to target activists. Activists have demanded that the state be more transparent about who conducts surveillance, who is targeted, and to what end.

In December 2011, Reflets, a French news site, published an investigation on the purchase of spyware from the French company Amesys Bull. The article refers to an investigation carried out by journalists from the Wall Street Journal who found that Amesys Bull sold spyware to the former Qadhafi regime in Libya. Reflets reports that the same spyware was sold to the Moroccan government and that engineers from Amesys Bull spent time in the country training government personnel for the use of such sophisticated spyware. The software, called Eagle, uses Deep Packet Inspection and is used to monitor emails, Skype conversations, and various encrypted materials.

Beyond these concerns, anonymity is broadly respected. Internet users do not need to register or provide any kind of identification at cybercafes. There are no indications that the purchase and use of encryption software by private citizens or companies is restricted. However, free access to the technology is starting to change. In the past, pre-paid SIM cards were purchased anonymously and citizens could get them from the three telecom companies’ retail stores without having to show identification. Today, customers are asked for a copy of their ID. However, street vendors and other non-affiliated sales outlets continue to provide SIM cards without IDs.

Intimidation and Violence

The threat of legal prosecution is often used to intimidate critical voices and curtail organizing around political causes. After the publication of interviews and investigations into surveillance practices in Morocco, Morocco’s interior ministry announced that a criminal complaint had been filed against “persons who distributed a report containing grave accusations about spying practices.” The report was published by Privacy International and Digital Rights Association (ADN), its Moroccan partner.

60 Interview with Zineb Belmkaddem.
61 Interview with Hisham Almiraat, conducted January 13, 2014.
63 Interviews with digital activists and online journalists.
67 Interviews with Dr. Fouad Abbou, professor of computer Science and Telecommunications and Dr. Hamid Harroud, director of the Information Technologies Services of Al Akhawayn University in Ifrane, conducted on 29 March 2015.
Authorities also use trumped up charges of drug possession, adultery, and others to intimidate well-known activists and journalists. Ali Lmrabet was denied paperwork necessary to renew his passport, residency, and work papers in mid-2015. In April 2015, with the expiration of a ten-year ban from publishing, he unsuccessfully attempted to restart his satirical news site DemainOnline. He subsequently went on hunger strike in front of the United Nations building in Geneva until the interior minister indicated he could receive his new passport.\(^69\)

**Technical Attacks**

Reports and interviews\(^70\) with prominent activists reveal an ongoing campaign by anonymous hacking groups to target outspoken voices. Groups such as the Monarchist Youth, the Moroccan Repression Force, the Moroccan Nationalist Group, and the Royal Brigade of Dissuasion have hacked into activists’ email and social media accounts, often publishing offensive content in a bid to harm their reputation.\(^71\)

In addition to surveillance and malware attacks, online news portals that express dissenting voices are subject to continuous cyberattacks. In one instance, Almiraat stated that his website was subjected to a cyberattack in July 2011 by a sophisticated computer virus.\(^72\) The site administrator had received an email that claimed to contain promising journalistic leads, such as videos of police misconduct. An investigation into the source and nature of the virus revealed that it was a Trojan Horse developed by Hacking Team, a company based in Milan, Italy. The virus downloads itself and hides among files, and can access contents on the computer, monitor in real time the use of the computer, log all the keys that are being hit, therefore giving away any passwords that are typed, and can activate the computer’s webcam and microphone and capture pictures and videos.\(^73\) The price of the software is estimated at €200,000 (US$220,000) and the company deals principally with governments and law enforcement agencies, leaving little doubt that the attacker was a law enforcement agency in Morocco.
Myanmar

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>19</td>
<td>18</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>25</td>
<td>28</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>60</td>
<td>63</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- International telecommunications companies Telenor and Ooredoo began providing mobile service in 2014, increasing the public’s access to affordable SIM cards outside the state-issued ration (see Availability and Ease of Access).
- The supply of SIM cards fell short of demand, fueling black market prices up to ten times the market rate; service quality remained poor (see Availability and Ease of Access).
- The Ministry of Communication and Information Technology released two regulatory laws but bureaucracy slowed enforcement, and even the state-owned firm failed to comply. Other promised legislation on cybersecurity has yet to materialize (see Regulatory Bodies and Legal Environment).
- The government detained and charged internet users for online activities, including three men jailed for two years each for insulting religion on Facebook (see Prosecutions and Detentions for Online Activities).
- Government officials pressured social media users not to distribute or share content that offends the military, or disturbs the functions of government (see Content Removals).
- Parliament temporarily suspended a five percent tax on mobile phone top-ups in May 2015 following protests on social media (see Digital Activism).
Introduction

Internet freedom in Myanmar declined during the coverage period of this report in comparison with the progress made since the country undertook liberalization in 2011. The government and security forces stepped up intimidation of internet users during social protests, intensifying conflict in ethnic minority regions, and during preparation for the 2015 national elections.

Since the political reform in 2011, telecommunications has become one of the most dynamic sectors in Myanmar. In 2013, the government granted two international telecommunications companies the opportunity to provide services and infrastructure alongside local firms. Besides creating jobs, the move drove much-needed legal reform. The government passed a Telecommunications Law drafted with input from the international community, and Norway’s Telenor Group established the country’s first independent connection to the international internet in March 2014. Qatar’s Ooredoo was the first to launch and offer a mobile phone service to a large part of Myanmar in August 2014. The Ministry of Communication and Information Technology (MICT) released two regulatory laws: “License Provision” in October 2014 and “Networking and Linking” in January 2015.

The government of former military leader President Thein Sein officially ended media censorship in 2012, and internet freedom improved in 2013, but the situation began to deteriorate since late 2014 as the practices of the old regime were revived. In addition to assaults and detentions, authorities employed legal, administrative, and other sanctions to influence content, and some clauses in the Telecommunications Law may allow censorship and surveillance. At the same time, the government amended, but failed to nullify, a 2004 Electronic Transaction Law which the junta notoriously used to criminalize political activism online.

Prior to 2014, internet access was only available through state-linked internet service providers (ISPs). They, too, are undergoing partial reform. The military-linked Yatanarpon Teleport (YTP) is transforming into a public company, but local news reports say government and military interests have purchased significant shares. Plans to privatize the state-owned Myanmar Post Telecommunication (MPT) have not materialized since they were announced in 2012.

Despite official commitments to good governance, military-owned conglomerates still appear to be manipulating the market. Since July 2014, the general public can access affordable SIM cards without needing to go through a state sponsored lottery, thanks to the international telecom companies, and mobile penetration has increased, though not enough to meet demand. Yet the internet lacks bandwidth to support the surge in online activity, and service quality remains poor because of inadequate infrastructure.

Online communication reflected political polarization developing in advance of 2015 elections. Opposition leader and Nobel Peace Prize laureate Aung San Suu Kyi of the National League for Democ-

---

1 Earlier Freedom House publications referred to Myanmar as Burma. The military-led government changed the country’s name from Union of Burma to the Republic of the Union of Myanmar without a referendum in 1989, a decision the opposition rejected as politicized. Myanmar became increasingly common, particularly after the regime adopted a more civilian form of government.


Myanmar

The National League for Democracy (NLD) party now serves in the parliament. However, she is barred from running for president in elections scheduled for 2015 under a clause in the constitution that excludes candidates who have a spouse or children who are foreign nationals. Aung San Suu Kyi had two sons with her late husband, Michael Aris, and both are British citizens. The 2008 clause was drafted with her in mind, her supporters believe, and digital campaigns were waged by those who sought to amend the clause and those who wished to retain it. Other grassroots campaigns, such as a movement promoting educational reform, also employed mobile apps to spread information about protests and other activities. The most effective outcry in social media that forced the state to review its policy came from online protests against the government’s imposition of five percent commercial tax on mobile top-ups starting from June 1st. Thanks to massive campaigns on social media, especially on Facebook, the parliament passed an urgent proposal to delay the tax until at least the end of the next fiscal year, on March 31, 2016.

The influence of rising religious nationalism also increased online. The government has maintained discriminatory policies against ethnic minorities like the Muslim Rohingya, who are denied citizenship under Myanmar’s law. Anti-Muslim hate speech was rampant online during the coverage period, overwhelming opposing campaigns that promoted tolerance. Since February 2015, the military has launched a military offensive against the armed Kokang ethnic group, which is based in the northeast along Myanmar’s shared border with China. This was accompanied by social media warfare framing the Kokang conflict as an infringement on state sovereignty from the outside power, China.

Obstacles to Access

Internet access is improving in Myanmar, as increasing numbers of users go online via cell phones, which is growing comparatively more affordable. Yet internet penetration still ranks among the world’s lowest. The quality of service remains poor because of inadequate infrastructure, and poverty continues to limit citizens’ internet usage.

Availability and Ease of Access

The number of internet users has notably increased over the past five years, but remains a fraction of the population, though precise figures are disputed. Internet penetration was at 2.1 percent in 2014, up from 1.6 in 2013, according to the ITU estimate, which experts in Myanmar considered low. Users in most provincial towns have much worse access in comparison with the few urban cities, let alone rural villages. Power outages, service interruptions, and inadequate numbers of transmission towers have made the conditions onerous.

Private internet connections are prohibitively expensive, though there is significant regional variation. The one-time installation cost of home broadband access from the MPT, the dominant state-owned provider, is US$50, plus an annual fee of US$50, but monthly rates range from US$17 to US$80, depending on speeds, which range from 512 Kbps to 2.5 Mbps. For a faster fiber-optic internet connection, setup costs from US$200 to US$1,000 and monthly service, starting at US$100, can run...

---

Myanmar

up to thousands of dollars per month for speeds up to 100 Mbps, in addition to an annual US$60 fee. Redlink, a private company run by the son of a former military general-turned-house speaker, charges even more. Users pay US$500 in setup costs, plus US$125 monthly and US$60 annual fees for a fiber-optic connection of 2 Mbps. Prices have fallen during the coverage period in comparison with previous years. However, since Myanmar’s gross domestic product was just US$980 per capita in 2014, these costs keep personal internet access far out of reach for the majority.

More people connect to the internet via mobile phones. During the coverage period, over 90 percent of internet users accessed the internet using a cellphone. Over 7 million people accessed the internet via mobile phone in December 2014, three times than the previous year. Just 120,000 internet users subscribed using ADSL or fiber-optic connections. In August 2014, the foreign telecom firm Ooredoo joined the market and sold its service charging US$1.50 per SIM card. In the following month, Norway-based Telenor started distributing its SIM cards in the market with the same price.

Mobile penetration in the country reached at least 30 percent in December 2014, an increase from 13 percent in 2013. Ministry of Communications and Information Technology figures cited by the ITU put mobile penetration at 49 percent in the same period. The figures may be misleading, since many people use more than one SIM card and subscribe to different service providers in order to beat connection issues. Sales of dual-SIM handsets are increasing, as it is standard for mobile internet users to purchase at least two SIM cards. Officials reported mobile penetration reached 55 percent by March 31, 2015. This calculation was based on the number of active SIM cards, which totaled 28.1 million.

Since the two foreign giants lack infrastructure compared to MPT, their underperforming services are often the impetus for users to spend more on dual connections, even while their presence in the market was expected to drive prices down. MPT has offered mobile phones since the 1990s, but charged from US$2,000 to US$5,000. The price dropped to US$200 in 2012 after the country entered a political and economic liberalization in 2011. In 2013, the military-owned MEC and MPT distributed a finite number of SIM cards per month for about US$1.50 each under a state-run lottery.

The state-owned MPT offers this more reliable service and coverage at a premium, in violation of the state’s own pricing regulation. According to an MCIT directive, operators should not charge more than MMK 20 per minute for phone calls during peak hours and MMK 15 per minute off-peak. But the MPT charges its users MMK 50 per minute for a phone call. Ooredoo and Telenor charge MMK 25 per minute, according to local news reports.

An MPT promotional “Swe Thahar” (Friendship) plan introduced in January began pricing internet by volume rather than duration, but it cost users MMK 15 per MB compared to MMK 10 under Telenor and Ooredoo, while per-minute phone rates are still higher than Telenor and Ooredoo’s. MPT users who have not signed up for the new Swe Thahar plan are not receiving the promotional pricing. In addition, the MPT did not offer its new plan to CDMA phone users. Users with CDMA phones paid

9 Based on an exchange rate of MMK 1,000 to US$1, fiber service for 100mbps was listed at MMK 7,000,000 in 2015. See, http://www.mpt.com.mm/en/product-services/fixed-line-internet/
Myanmar

from US$500, at the official rate, to as much as US$5000 on the black market since the connection option was first available in 2000, and view their exclusion from more affordable pricing plans as discriminatory.

In total, a regular mobile internet user might spend MMK 10,000 to 20,000 (US$10 to US$20) per month, while those who rely on it for business spend from 30,000 to 50,000 (US$30 to US$50). This represents little change from last year and limits connectivity for a large percentage of the population since one quarter of the people remains below poverty line. 15

Restrictions on Connectivity

Until 2014, the Ministry of Communications and Information Technology (MCIT) essentially controlled the country’s infrastructure via the state-owned MPT, which covers over 90 percent of the country and is continuing to expand with a US$2 billion investment from Japan’s KDDI Corp and Sumitomo Corp. 16

Myanmar is connected to the international internet via the SEA-ME-WE 3 submarine cable, and satellite and cross-border cable links with China and Thailand. China Unicom and MPT signed a Memorandum of Understanding in July 2013 to build a link from the SEA-ME-WE 5 cable through Mandalay and into China. 17 The construction of the cable is in progress and expected to be in use by late 2015. Though both foreign firms are planning to establish their own cable links to Thailand, they so far share the MPT’s backbone to connect with the international internet. Even if they could connect to the international internet in 2015, they would only serve users with a 10 GB bandwidth connection, while the MPT now provides 32.32 GB to its users, a significant increase from 3.92 GB in 2010-2011. 18 Low bandwidth is largely responsible for the congestion experienced by local internet users, especially during peak afternoon hours. Power outages also frequently disrupt access. 19

In late 2014, an MCIT spokesperson noted that there have been some discussions with international experts and consulting firms, including Price Waterhouse Cooper, about MPT privatization. Thus far, the connection to the international internet is essentially controlled by the state-owned MPT.

In October 2014, the MPT stopped accepting new applications for fiber-optic internet service. Since all ISP firms operate under the MPT, they also could not provide internet service to new customers. The stated reason for this service suspension for new users was that the MPT plans to expand bandwidth, and the service will be extended to new customers in 2015. 20

In some areas, Mabatha monks attempted to disrupt installation of transmission towers by Ooredoo because the firm has its roots in a Muslim country. In one June 2015 incident in Rangoon, monks took down Ooredoo’s advertisement boards from public lampposts. The group announced a boycott


Interview with two managers from local ISPs in November 2014.
Myanmar

of the company after it was granted an operating license in 2013, denouncing anyone working for Ooredoo, or using their services, as a traitor.

**ICT Market**

Despite progress in diversifying the market, state-owned conglomerates continue to skew the telecommunications playing field through two main ISPs,\(^{21}\) the state-owned Myanmar Post Telecommunication (MPT), and the military-linked Yatanarpon Teleport (YTP). Redlink, SkyNet, and other FTTH providers operate under YTP.

In 2012, the government announced plans to liberalize its telecom sector and invite foreign investment.\(^{22}\) In June 2013, the government awarded international licenses to Norway’s Telenor and Qatar’s Ooredoo, allowing them to offer services and infrastructure alongside the state-owned MPT.\(^{23}\) In April 2015, the MCIT announced that it would award an operator license to the fourth telecom firm, Royal Yatanarpon, which was once the military-linked local firm YTP that is now being transformed into a public company. Royal Yatanarpon is reportedly planning to enter the market in partnership with Vietnamese military-linked Viettel Group, which is preparing to invest US$1.8 billion in the Burmese telecommunications sector.\(^{24}\) Up until late March 2015, the government has granted 19 local and foreign firms licenses to provide telecommunication services.\(^{25}\) The government announced in 2012 that the MPT would be privatized in a few years, but nothing concrete was done in past few years.

**Regulatory Bodies**

The Posts and Telecommunications Department regulates Myanmar’s telecommunications industry under the MCIT. Under the junta, the MCIT and intelligence agencies implemented arbitrary and ad hoc censorship decisions. Other state institutions tasked with information and communications technology (ICT) development and management are largely inactive.\(^{26}\) The Myanmar Computer Federation, formed under the 1996 Computer Science Development Law and comprised of industry professionals, is the designated focal point for coordination with the ITU. Critics say it failed to take advantage of the 2011 political change to play a more active role in the ICT sector.

Clause 86 of the Telecommunications Law established an independent commission to take over regulatory functions within two years. The business community also welcomed the law’s creation of an appeal tribunal mechanism to adjudicate over administrative issues in the telecommunications

---

21 Many still refer to the Ministry, formerly responsible for Communications, Posts and Telegraphs, by its old abbreviation MPT.
26 These include the Myanmar Computer Science Development Council, the e-National Task Force, the Myanmar Computer Federation, the Myanmar Computer Professionals’ Association, the Myanmar Computer Industry Association, and the Myanmar Computer Enthusiasts’ Association.
Myanmar

industry. The MICT released two regulations expanding on the telecommunications law during the coverage period, a License Provision on October 14, 2014, and a separate one on Networking and Linking in January 6, 2015. The enactment of the by-laws and regulations is a good indication of the government’s willingness to further liberalize the country’s telecommunications sector. However, bureaucratic processes are still blocking implementation.

Limits on Content

During the coverage period, the military actively pressured online media users and outlets not tarnish its reputation and public image. While digital content was not subject to censorship, sensitive political and social topics were nevertheless underrepresented online. Myanmar’s failure to remove restrictive punishments for online content occurred in the context of a deliberate government campaign to marginalize balanced and dissenting voices. Tactics included economic pressure on independent media, manipulative political commentary, and tacit encouragement of nationalistic hate speech against the Muslim minority.

Blocking and Filtering

The government lifted systematic state censorship of traditional and electronic media in 2012. Since then, political content appeared to be almost universally available, and even social content, such as pornography, was not blocked as of mid-2015.

Content Removal

While content remained available and accessible for new readers in theory, authorities made a concerted effort to exclude certain topics from mainstream discourse in ways that lacked transparency and due process.

Notably, the military pressured individual online users and media outlets not to damage the public image of the armed forces. In one instance, the military released a statement protesting the private weekly Myanmar Times journal for publishing a cartoon that “insulted the dignity of the armed forces,” and prompted a takedown and apology from the journal. The cartoon, published in the March 25 edition, featured a husband and wife talking about the ongoing conflict between the military and ethnic Kokang insurgents. The husband relays that the army had taken the hills, to which the wife replies “aren’t they satisfied with taking the farms?”27 The military also released a statement on April 26 targeting the Eleven Media group for publishing a news article about military losses in a battle with the Kokang. The Armed Forces Accurate Information Team said the article breached journalistic ethics and harmed the dignity and spirit of military personnel.

Media, Diversity, and Content Manipulation

In this climate, self-censorship remains common online on military and related issues. While some topics are discussed more freely since liberalization, internet users are reluctant to discuss past abus-

Myanmar

es for fear of jeopardizing the political opening. On May 3, the military sent a warning letter to the Myanmar Press Council stating that the local news media outlets were not to cover any statements released by Kokang ethnic armed group. The letter warned that any media outlet that fails to follow the instruction will face action in accordance with the existing laws.  

Social media and communication apps, including Viber, Tango, Friendfinder, and Google+, are freely available. In September 2014, the speaker of the Upper House even arranged for members of parliament to install Viber to communicate with one another and with their constituencies. MPs in the same political party or with similar view on particular issues set up Viber groups to exchange information. In June 2015, when the Burmese currency value dropped to a record low of MMK 1,105 to the dollar and MMK 1,235 on the black market, Thura Shwe Mann, who is the speaker of the Lower House, invited Facebook users to make suggestions—and actually implemented some of them.

Facebook is the most popular social media platform, since many users developed the habit of using the platform to share information, initiate collective action on social and political issues, or follow exile media outlets when website blocking was still pervasive. According to one estimate, there were three million Facebook users in Myanmar in January 2015. (In better-connected Thailand, the number of Facebook users was estimated at 28 million.) For some users frustrated with the challenge of navigating between sites on poor connections, Facebook is the sole source of online news, potentially depriving local outlets of the advertising revenue that would reduce their dependence on state-operated print outlets.

Some progovernment blogs, such as OppositEye, actively manipulate online commentary to launch smear campaigns against Muslims or the political opposition.

Ethnic Burman internet users also spread racially-charged comments across social media platforms throughout the coverage period. A radical group of Buddhist monks named Mabatha has intensified its anti-Muslim campaign in this coverage period. In January, the best-known leader of the group, Ashin Wirathu, called a UN special envoy a “bitch” and a “whore,” comments which were widely shared by extremists and military-hired cyber troopers. A Facebook page in Wirathu’s name has thousands of supporters. He even created his own news app to propagate hate speech, but the authorities thus far have not taken any action against him or other hatemongers online.

In contrast, the persecuted Rohingya minority lack a domestic online audience, though some Rohingya bloggers and Facebook users have gained recognition overseas. Individuals or news outlets that provide even neutral coverage of religious tensions are accused of anti-Burmese bias.

Digital Activism

---

30 “Facebook domestic consumption more than the three neighboring countries and at six percent,” The Internet Journal, January 22, 2015, http://www.internetjournal.media/new/1254
33 “UN condemns Myanmar monk Wirathu’s ‘sexist’ comments,” BBC News, January 22, 2015, http://bbc.in/1E4GBDA
Myanmar

In 2014, Buddhist nationalists successfully campaigned to force the government not to allow the Rohingya minority to register their ethnic identity in a 2014 census sponsored by the United Nations Population Fund. In early 2015, the government also conceded to their demand to disenfranchise over one million people, largely Rohingya and other minority groups, by revoking their temporary registration certificates, known as white cards. In both online and off-line campaigns, nationalists also campaigned extensively during the coverage period to legislate bills to “protect” race and religion. In March 2015, the Lower House passed the Population Control bill, which requires mothers to have their children three years apart. Observers feared it would be implemented selectively to withhold rights from children born in minority communities. The Buddhist Women’s Special Marriage bill, requiring Buddhist women to seek permission from local authorities before marrying a man of another faith, was also passed in the lower house. The Buddhist nationalist movement is also urging the government not to amend Clause 59F of the constitution, which bars Aung San Suu Kyi from becoming a presidential candidate in the 2015 election.

Campaigns to counter these negative online campaigns also had some success. The Panzagar, or “Flower Speech,” movement opposes the spread of anti-Muslim sentiment and has gained media attention and popular support. It was set up by Nay Phone Latt, the blogger and director of the technology and free speech advocacy organization Myanmar ICT for Development Organization (MIDO), who spent nearly four years in jail for writing about the crackdown on monk-led protests in 2007. In February 2015, the movement distributed “Speak Panzagar” stickers of 24 cartoon characters voicing Burmese-language slogans such as “Don’t spread hate” and “Don’t fuel conflict” for free download on Facebook and Viber. These stickers became very popular among internet users, and MIDO plans to make more representing different ethnic culture and languages and to make them available in six other countries with large minority populations from Myanmar, such as Singapore, Thailand, and the United States. In January 2015, MIDO and the U.S Agency for International Development (USAID) jointly organized a three-day long forum called “Peace Tech Exchange” where more than 100 groups joined and discussed how to stop hate speech with the help of technology.

Online campaigners also opposed a government-initiated five percent tax on mobile phone top-up cards announced on May 18, 2015, with some success. The tax was suspended on May 27 until the next fiscal year.

Violations of User Rights

The October 2013 Telecommunications Law transformed the industry, but failed to repeal harsh punishments for political dissent on electronic media. Journalists conducting online and off-line reporting on student protests and police crackdowns were harassed, attacked, and detained by police. Increasing

42 Kyaw Hlaing, “Hate speech technology in order to deter more than 100 organizations to discuss collectively,” The Internet Journal, January 15, 2015, http://internetjournal.media/new/1155.
numbers of traditional media journalists were arrested during the year, contributing to a climate of intimidation online. Ten journalists were imprisoned in 2014 and 19 were facing trial, and Myanmar was the 10th worst jailor of media workers in 2014 according to the Committee to Protect Journalists. In addition, hackers targeted the Eleven Media news website for “slandering the government.”

Legal Environment

The current constitution, drafted by the military-led government and approved in a flawed 2008 referendum, does not guarantee internet freedom. It states that every citizen may exercise the right to “express and publish their convictions and opinions,” if “not contrary to the laws enacted for Union [of Myanmar] security, prevalence of law and order, community peace and tranquility or public order and morality.”

Parliament enacted the long-pending Telecommunications Law, drafted with the help of international experts including the World Bank, in October 2013. Domestic and international investors applauded the consultative drafting process, along with the guidelines for the industry, which provided the foundation for improving access. In fact, the telecommunication law itself failed to repeal the notorious Electronic Transaction Law (ETL) of 2004, which has routinely been used to criminalize digital activism. Instead, parliament amended the ETL, reducing but not eliminating possible jail sentences for ill-defined online actions.

Under the newly-amended ETL, “any act detrimental to” state security, law and order, community peace and tranquility, national solidarity, the national economy, or national culture—including “receiving or sending” related information—is punishable by 3 to 7 years imprisonment, down from 7 to 15 years. The Telecommunications Law itself also includes broadly-worded clauses that subject internet activity to criminal punishment. Clause 68 punishes “communication, reception, sending, distribution or sharing of incorrect information with dishonest intention” with imprisonment for up to a year, an unspecified fine, or both. Given Myanmar’s history of violating user rights, these broadly-worded legal provisions are a matter of concern for internet freedom. In 2014, Thaung Tin, an MCIT deputy, acknowledged the need to fix repressive laws like the ETL and the Computer Science and Development Law, which criminalizes unauthorized use of a computer with a “fax-modem card.”

Laws regulating e-commerce and combatting cybercrime are also anticipated, though the timeframe is unclear. In December 2014, the MCIT said that they are revising the ETL in order to clarify confusing language and will be presenting their draft to the public for discussion soon.

Prosecutions and Detentions for Online Activities

Dozens of political prisoners formerly jailed for electronic activities remain free after they were released en masse in 2011. Though the release was described as an amnesty, they were generally not...
acquitted, but rather released on condition that reoffenders will receive a new sentence in addition to previously unfinished sentences. At least three former military or government officials remain imprisoned after they were sentenced in early 2010 for leaking sensitive information about junta activities to overseas groups using digital tools.48

In late February, police arrested freelance photojournalist Aung Nay Myo for uploading a satirical post on Facebook mocking the president’s relationship with the military. The Facebook post depicted President Thein Sein and military commander general Min Aung Hlaing photoshopped into a poster for a movie known as military propaganda.49 Though he was released after three days of detention, the interrogators forced him to turn over his password and take down the post. In news reports, authorities were quoted threatening those who shared the post with legal measures.

In March, a court in Rangoon jailed one New Zealander and two Burmese for two years each on charges of “insulting religion” in a promotional Facebook post depicting a photoshopped picture of the Buddha wearing headphones and sunglasses. The men were arrested in 2014 after members of the Association for the Protection of Race and Religion (Mabatha) complained to authorities.50 The picture, which advertised a bar, was taken down the day it was posted.

On March 10, 2015, at least two journalists were arrested while covering a crackdown on student protests in central Myanmar. In a separate incident, two reporters covering labor protests in Rangoon were also briefly detained on March 4.51 All four journalists reported for media organizations who publish in both print and online formats. The case of a citizen journalist who was fatally shot in military custody in October 2014 has yet to be solved.

Increasing numbers of traditional media journalists were arrested during the coverage period. At least 10 journalists were imprisoned and 19 were facing trial in 2014, making Myanmar the 10th worst jailor of media workers worldwide.52 Journalists and online users who criticize or investigate military matters are frequently charged with national security-related laws such as the colonial-era 1923 Official Secrets Act and defaming the state or the court. In July 2015, the government sued 17 editors from the Eleven Media group with contempt of the court in the Mandalay Region Court.

**Surveillance, Privacy, and Anonymity**

State surveillance, historically pervasive and politicized, abated after the political opening, but intensified somewhat in 2013 due to religious unrest and the opposition-led constitutional reform movement, among other issues. Regrettably, the Telecommunications Law introduced greater scope for abuse. Clause 75 grants unspecified government agents the authority “to direct the organization concerned as necessary to intercept, irrespective of the means of communication, any information that affects the national security or rule of law.” The clause added that the government would do so

---

48 In January 2010, a former military officer and a foreign affairs official were sentenced to death, and another foreign affairs official was sentenced to 15 years in prison, for leaking information and photographs about military tunnels and a general’s trip to North Korea. Interview with Bo Kyi, cofounder of the Association for Assisting Political Prisoners (Myanmar), July 2012. The executions have not been carried out.


Myanmar

without affecting the fundamental rights of the citizens, but included no privacy protections. Clause 76 allows the government to inspect or seize this information on the premises of private telecommunications enterprises.

Telenor requires SIM card registration in compliance with local regulations. In November 2013, however, Telenor announced that it would protect its customers from government wiretapping, and asked information officials for clarification about interception rules and procedures. But the firm’s CEO, Petter Furberg, told media in May 2015 that Telenor was pressed by the authority to disclose phone records and locations of some users. Pending clarification to the law, the firm assessed requests on a case by case basis, complying with 3 out of 15 intercept requests it described as “serious drug offenses, terror threats, and missing persons.”

Ooredoo told journalists it will prevent any wiretapping of its phone networks. But several international and local civil society representatives and some diplomats believe that the military has stepped up surveillance by means of wiretapping, hacking, and even intercepting Voice over Internet Protocol (VoIP) calls amid the intensifying social protests and political rivalries developing during the coverage period.

Intimidation and Violence

Journalists and bloggers periodically face attacks in Myanmar, though no attacks targeting internet users were publicized during the reporting period. In one example on March 10, 2015, police beat several journalists with batons and stones, including a foreign photographer, as they covered a police crackdown on student protests in central Myanmar.

Technical Attacks

On October 2, 2014, hackers attacked the English-language site for The Irrawaddy magazine, in apparent reprisal for its coverage of meetings between Buddhist-nationalist groups, including controversial monk U Wirathu, and their Sri Lankan counterparts. In April 2015, Eleven Media’s website was attacked by hackers, who linked to Executive Editor Nay Htun Naing’s Facebook profile from the main page of the website. The attack took place after the publication uploaded Nay Htun Naing’s article responding to President Thein Sein’s top economic adviser, who had lambasted the journalist for “declaring jihad” on the government through his coverage of deteriorating economic conditions.

55 Interviews with three senior INGOs staff, five local NGOs chief, one senior ruling party leader and two diplomats.
Nigeria

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>33</td>
<td>33</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- The regulator shut down an SMS shortcode used by the All Progressives Congress opposition party to fundraise during the electoral campaign season in February 2015, which critics saw as politically motivated (see Content Removal).

- Digital activism played a significant role during the March 2015 general elections, helping candidate Muhammadu Buhari defeat incumbent President Goodluck Jonathan, who was widely criticized on social media for his inefficacy (see Digital Activism).

- In February 2015, a local Reuters correspondent was arrested on trumped-up allegations of espionage and planning to “send negative reports to the outside world,” which observers believe was part of the government’s efforts to obstruct international media from covering the general elections (see Prosecutions and Detentions for Online Activities).

- The Cybercrime Act 2015 signed into law in May 2015 includes provisions that threaten to violate citizens’ rights to privacy (see Surveillance, Privacy, and Anonymity) and freedom of expression (see Legal Environment).

- The independent news outlet Premium Times experienced a DDoS attack during its presidential election coverage (see Technical Attacks).
Nigeria

Introduction

In 2014 and 2015, a growing number of Nigerians had access to the internet and other information and communications technologies (ICTs) due to an increase in mobile phone data services and improved broadband. Compared to the environment for traditional media in Nigeria, online media was relatively free from restrictions, with no blocking or filtering of online content reported during the coverage period.

Social media played a significant role during the general elections held in March 2015, providing a platform for digital activism that drew widespread attention to President Goodluck Jonathan’s inefficacy. In response, government authorities tried to limit internet freedom in haphazard ways. In February 2015, for example, the regulator shut down an SMS shortcode used by the All Progressives Congress opposition party to fundraise during the electoral campaign season, which critics saw as politically motivated. Also in February, a local Reuters correspondent was arrested on trumped-up allegations of espionage and planning to “send negative reports to the outside world,” which observers believe was part of the government’s efforts to obstruct international media from covering the general elections. And in March, the independent news outlet Premium Times experienced a massive DDoS attack during its presidential election coverage. Meanwhile, an alarming number of violent attacks against traditional media journalists by both the Nigerian security forces and militant groups led online journalists to be more cautious than usual in their coverage of the elections.

Nigerian users remained concerned about growing online surveillance in the past year, even as the government continued its push to make ICT tools more available to citizens. Suspicions of the government’s surveillance capabilities increased following the publication of leaked emails from the Italian surveillance company Hacking Team in July 2015, which revealed that the government of Bayelsa state had an active contract with the company from 2012 to November 2013. In May 2015, outgoing President Goodluck Jonathan signed the Cybercrime (Prohibition, Prevention, etc.) Act 2015 into law, providing a long-awaited framework for addressing the country’s notorious cybercrime epidemic. The law, however, includes provisions that threaten to violate citizens’ rights to privacy and freedom of expression.

Obstacles to Access

Access to ICTs continued to grow, despite high costs and frequent power cuts that disrupt network services. There were no restrictions on connectivity, in contrast to the previous coverage period when mobile phone networks were cut off in three northeastern states due to emergency rule.

Availability and Ease of Access

The internet in Nigeria has continued to spread rapidly, particularly with the proliferation of mobile phone data and Fixed Wireless Access (FWA) services. According to the Nigerian Communications Commission (NCC), the sector regulator, there were over 83 million active mobile internet subscriptions on GSM and CDMA networks as of February 2015. The International Telecommunication Union

1 Fixed Wire Access (FWA) is a type of high-speed internet access that uses radio signals as a connection to service providers instead of cables, enabling areas that lack fiber optic cables or DSL to access broadband internet.
2 Nigerian Communications Commission, “Active Internet Subscriptions (GSM) and (CDMA),” accessed March 31, 2015, http://www.ncc.gov.ng/
Nigeria

(ITU) estimates that 43 percent of Nigerians had access to the internet in 2014, up from 38 percent in 2013, while 78 percent had access to mobile phone services, increasing from 73 percent in 2013. By contrast, the NCC reported a mobile phone teledensity of 102 percent as of February 2015.

Increasing access to the internet is driven by internet-enabled mobile handsets that provide affordable bundled data services to mobile subscribers. For example, as of April 2015, BlackBerry service packages cost as low as US$7.50 a month, an option that attracts many young Nigerians. As technologies improve, prices are continuing to decrease; in 2015, for example, the average cost of a GSM plan cost US$0.26 per megabyte of data, compared to US$1 per megabyte in 2011, while FWA services cost an average of US$37 per month, down from US$63 per month in 2014. Accessing the internet at a cybercafe costs about US$0.55 per hour, down from US$0.63 per hour. Nevertheless, these costs are still a major impediment to internet access for many Nigerians, particularly those in rural areas. In addition, the quality of service remains poor, with users frequently complaining about their inability to enjoy seamless data services. Internet speeds are slow, averaging 2.8 Mbps (compared to a global average of 4.5 Mbps), according to May 2015 data from Akamai’s “State of the Internet” report.

Power cuts frequently disrupt service and access, with many users reporting the need to use private generators to stay online during outages, despite the country’s status as an oil-rich country. In the first quarter of 2015, Nigerian households reportedly received an average daily cumulative power supply of between five and seven hours per day, leading over 77 percent of Nigerians to rely on alternative electricity sources.

Telecommunication companies also depend on diesel-powered generators to maintain consistent service amid sporadic power cuts, spending an estimated NGN 177 billion (US$1.14 billion) annually on fuel for the generators needed to provide back-up power for the country’s 22,000 base stations. Moreover, the need to pay for expensive backup power generators has accelerated the closure of cybercafes that were already struggling with competition against the growing popularity of internet access on mobile devices.

Restrictions on Connectivity

Nigeria is connected to the international internet via a number of submarine fiber-optic cables, and there are several competing national fiber-optic backbone networks in place, representing a vibrant and competitive telecommunications market that is not highly vulnerable to government interference.

Nevertheless, as part of an emergency directive imposed to fight Boko Haram in the northeastern...
Nigeria

states of Borno, Adamawa, and Yobe, the former government under President Goodluck Jonathan deliberately cut off access to mobile phone networks between May and December 2013 and again in March 2014 for about 20 hours. Residents complained of hardship due to the lack of telecommunications services and argued that the shutdown did little to stop the terrorist threat. Instead, the shutdown at times put citizens in harm’s way. For example, residents travelling to another city in search of mobile phone connectivity were reportedly ambushed and killed by Boko Haram militants. In November 2014, the government sought a six-month extension for emergency rule in the region but was rejected by both chambers of the National Assembly.

ICT Market

The ICT market in Nigeria has expanded considerably over the past decade, with the number of licensed internet service providers (ISPs) rising from 18 in 2000 to 189 as of the end of March 2015. There are also 11 FWA providers and 4 GSM mobile phone operators that provide internet access to their subscribers. Nevertheless, the growth of ISPs and FWA providers has slowed in recent years with the rise in mobile access. As of February 2015, the four privately owned GSM companies—MTN, Globacom, Airtel, and Etisalat—had a total of over 136 million subscribers between them.

Regulatory Bodies

The 2003 Nigerian Telecommunications Act vests regulatory responsibilities over the ICT sector in the Nigerian Communications Commission (NCC). Although the government nominates the NCC’s nine-member board of commissioners, the regulator’s decisions have been viewed as relatively independent. However, recent incidents—namely, the suspension of an SMS shortcode used for opposition fundraising during the election (see “Content Removal”)—has called the regulator’s independence into question.

All ISPs must obtain a license from the NCC to operate, and there have been no reports of any ISP being denied a license or registration renewal. However, new ISPs seeking to enter the market have faced stiff competition from larger ISPs and investor focus on the mobile sector. Meanwhile, the process of issuing GSM licenses is regarded as transparent. Unlike other auctions that are usually subject to political interference, most stakeholders have found GSM license auctions to be fair after those with political connections lost out in the process.

15 75 of which have licenses in need of renewal, according to the NCC website, which could mean that renewed license details have yet to be uploaded to the website, or that the regulator is in the process of renewing licenses. See: Nigerian Communications Commission, “Internet Services,” accessed March 31, 2015, http://bit.ly/1b4JUuw.
Nigeria

Limits on Content

No blocking or filtering of online content was reported during the coverage period, though the communications regulator shut down an SMS shortcode used by an opposition party to fundraise during the elections period. The campaign season also saw an uptick in progovernment commentators who were suspected of deliberately manipulating the information landscape on social media networks. Hashtag activism became a highly influential tool for citizens to draw attention to important issues and demand government accountability.

Blocking and Filtering

Online media is generally free from restrictions in Nigeria, and to date, the authorities have not carried out any blocking or filtering of content. The complex nature of Nigeria’s internet infrastructure makes it difficult to carry out systematic filtering or censorship. Nonetheless, Blue Coat’s Packet-Shaper appliance—a device that can help control undesirable traffic sent via online applications by filtering according to content category—was discovered in January 2013 on a private ISP in Nigeria, which was disconcerting to observers given the use of Blue Coat technology by the authorities in countries such as China, Bahrain, and Russia. No abuses of the filtering device have been reported.

YouTube, Facebook, Twitter, and various international blog-hosting services are freely available and among the most popular websites in the country. In the past few years, however, a few high-level government officials have made statements calling for a clampdown on social media, ostensibly as a response to the growing influence of critical commentary on the internet. Some citizens have viewed these statements as signs of impending online censorship.

Content Removal

The government did not issue any takedown requests, nor did it force content to be removed from the internet during the coverage period. Nevertheless, with the rise of anti-gay sentiments following the passage of the repressive Same Sex Marriage (Prohibition) Act in January 2014, LGBTI individuals reported increasing concerns over having content related to sexual orientation and gay rights targeted for removal by the NCC. As such, many LGBTI content creators have opted to host their websites on platforms based in the United States and Europe to avoid potential censorship.
**Nigeria**

In a murky case, the communications regulator in February 2015 shut down an SMS shortcode—a phone number with fewer digits to make it easier for users to remember—used by the All Progressives Congress opposition party to fundraise in the lead-up to the March 2015 general elections, claiming a violation of its established guidelines. 24 Though there was no evidence that the SMS shortcode block was politically motivated, Nigerian government agencies are known to align with the sitting president in order to retain the administration’s favor. In a positive step, a Federal High Court ruled in favor of the opposition party in March and awarded NGN 500 million (US$ 2.5 million) as damages against the regulator “for unlawfully banning the party’s presidential campaign fund-raising platform.” 25

**Media, Diversity, and Content Manipulation**

Nigeria is home to a diverse blogosphere, which has become an important platform for discussion and a source of reliable news for many users, providing a space for lengthy debate on a broad array of political and social issues among online commentators. Popular blogging platforms include Global Voices, Blogger, and WordPress.

Diverse political viewpoints are represented on Nigerian websites and blogs. Government efforts to manipulate online content are sporadic, though observers have noted a sharp increase in the volume of progovernment responses to citizens’ comments on social media in recent years. In addition, the growing number of suspicious Twitter users that actively attack critical voices has led some to believe that the government may be financing an army of online trolls to influence the online information landscape. In November 2013, progovernment trolls were suspected of blocking links to articles posted on the Facebook page of the well-known investigative online news outlet, Premium Times, by repeatedly reporting the links as abusive. Efforts to unblock the Premium Times’ links succeeded months later in January 2014. 26

Users practice a degree of self-censorship online but have become more open in discussing issues that were previously unpopular or taboo, such as gay rights, in recent years. In Nigeria’s growing anti-gay climate, however, many LGBTI individuals have reported feeling unsafe expressing themselves online using their real names and instead engage with the internet anonymously. 27 Online journalists were also more cautious than usual in their coverage of the March 2015 elections given the alarming number of violent attacks against traditional media journalists by both the Nigerian security forces and militant groups at the time. 28

**Digital Activism**

As active social media users, Nigerians have increasingly initiated campaigns on social media to call for social or political change. Following the abduction of over 200 schoolgirls by Boko Haram...

---

Nigeria

in April 2014, the hashtag #BringBackOurGirls became an international social media campaign that put a spotlight on the Nigerian government's haphazard and ineffectual response to the crisis. The widespread attention on the government's inaction garnered by the campaign led to a dramatic drop in President Jonathan's already waning popularity, costing him in the 2015 elections. While the Jonathan government ultimately failed to rescue the abducted girls, the campaign illustrated how hashtag activism has become a highly influential tool for citizens to draw widespread attention to important issues, demand government accountability, and punish erring governments with defeat at the polls.

Violations of User Rights

The Cybercrime Act 2015 signed into law in May 2015 includes provisions that threaten to violate citizens' rights to privacy and freedom of expression. A Reuters correspondent was arrested in February 2015, which observers believe was part of the government's efforts to obstruct international media from covering the general elections. The independent news outlet Premium Times experienced a DDoS attack during its presidential election coverage.

Legal Environment

Nigeria's 1999 constitution guarantees freedom of expression and the press, and the implementation of Sharia (or Islamic) law in 12 northern states has not affected internet freedom in those regions to date. Nonetheless, libel remains a criminal offense in Nigeria and may be broadly applied to online content, with the burden of proof resting on the defendant. Print media journalists covering sensitive issues such as official corruption and communal violence are regularly subjected to criminal prosecution.

In May 2015, outgoing President Jonathan signed the Cybercrime (Prohibition, Prevention, etc.) Act 2015 into law, providing a long-awaited framework for addressing the country's notorious cybercrime epidemic. The law, however, includes provisions that threaten to violate citizens' rights to privacy (see “Surveillance, Privacy, and Anonymity”) and freedom of expression. Under section 26 of the law, individuals can be criminally penalized for expressing or distributing "racist or xenophobic material to the public through a computer system or network" with up to five years in prison, a fine of up to NGN 10 million (US$50,000), or both.

State government officials in Nigeria have also made efforts to restrict freedom of expression within their jurisdictions. In March 2013, for example, the governor of the southern state of Bayelsa introduced a bill to the state assembly that aimed to criminalize "rumor mongering" and the spread of false information. While the bill remained stalled as of mid-2015, it did not deter the state governor from cracking down against alleged rumor mongering online, arresting one individual in October 2013 for a Facebook post criticizing the governor.

Nigeria

In an effort to codify protections for internet freedom, a coalition of civil society organizations released a draft Digital Rights and Freedom Bill in April 2015 to be introduced to the 8th National Assembly in 2015.

Prosecutions and Detentions for Online Activities

The Nigerian authorities occasionally arrest online journalists and ordinary users for their online activities. One arrest was reported during the coverage period.

On February 15, 2015, state security officers broke into the home of Reuters correspondent Tife Owolabi, arresting him on allegations of espionage and planning to “send negative reports to the outside world.” The authorities also seized his electronic devices—including cameras, laptops, hard drives, and an iPad. Though he was ultimately released and dismissed of all charges, the timing of his arrest coincided with other government efforts to obstruct international media from covering the March 2015 elections.

In September 2015, a blogger was arrested for a Facebook post that accused the wife of the Ogun state governor of laundering money. With a case set for late October 2015, blogger Ojo Emmanuel faces charges of criminal libel and conspiracy against the state government.

Surveillance, Privacy, and Anonymity

Thus far, there has been no evidence that the Nigerian authorities proactively monitor internet and mobile phone communications, but many online journalists have long suspected that they are being monitored by the state. News of the government’s acquisition of mass surveillance equipment over the past few years has deepened these suspicions. In July 2015, leaked emails from the Italian surveillance firm Hacking Team revealed that the company had a contract with the Bayelsa state government that expired in November 2013. The active period of the contract from 2012 to 2013 coincides with the state governor’s efforts at the time to crackdown on so-called “rumor mongering” online that led to the arrest of one Facebook user (see “Legal Environment”).

Earlier in April 2013, the online newspaper *Premium Times* published a report revealing that the federal government had awarded a secret contract to Israel-based Elbit Systems to help monitor internet communications in Nigeria. While the installation of the system was reportedly expected within

---

36 Outside of coverage period.
two years,\textsuperscript{41} there has been no further news of the system’s implementation as of October 2015. In April 2013, Citizen Lab research also found a FinFisher “Command and Control” server, which communicates with malware that can be used for surveillance, located on a private ISP.\textsuperscript{42} As of mid-2015, the extent to which such surveillance systems have been implemented is still unknown.

Other government surveillance efforts were revealed in the publicly available summary of the federal government’s 2014 budget proposal, which budgeted NGN 415 million (US$2.6 million) for a “Data Retention System,” NGN 359 million (US$2.2 million) for a “GSM Passive Off-the-air Interception System,” and NGN 350 million (US$2.2 million) for a “Strontium Sky Diligent Recon System” under the Directorate of State Security Services.\textsuperscript{43} While the exact purpose of these technologies is still unclear, and it remains unknown whether the systems have been purchased and installed as of mid-2015, the budgeted expenses increased suspicions of the government’s intent to enhance its surveillance capabilities, particularly amid frequent assertions by government officials of the need for technologies to fight the threat from Boko Haram.

Still under active discussion as of mid-2015,\textsuperscript{44} a draft Lawful Interception of Communications Regulation, introduced by the communications regulator in February 2013,\textsuperscript{45} has been criticized for bypassing the legislative process and lacking judicial safeguards against abuse or opportunities for redress, threatening to infringe on citizens’ constitutional right to privacy.\textsuperscript{46} If implemented, the regulation has conditions for interception both with and without a warrant and will require mobile phone companies to store voice and data communications for three years. It will also direct licensees to, on demand, “provide the National Security Adviser and the State Security Service with the key, code, or access to the Protected or Encrypted Communication.”\textsuperscript{47}

Meanwhile, requirements on service providers to retain user data and intercept electronic communications are included in the latest Cybercrime Bill, implemented in May 2015.\textsuperscript{48} Under section 38 of the bill, providers are required to “keep all traffic data and subscriber information...for a period of two years” and comply with requests from law enforcement agencies to access this data.\textsuperscript{49} Judicial oversight of these requirements is unclear.\textsuperscript{50}


\textsuperscript{42} Morgan Marquis-Boire et al., \textit{For Their Eyes Only: The Commercialization of Digital Spying}, Citizen Lab, April 30, 2013, \url{http://bit.ly/1amNwJ1}.


\textsuperscript{44} Paul Adepoju, “Nigeria: communications regulator to legalise interception,” \textit{Web Africa}, July 16, 2015, \url{http://bit.ly/1RdfHj8}.


\textsuperscript{47} Nigeria Communications Commission, “Draft Lawful Interception of Communication Regulations.”

\textsuperscript{48} “Nigeria’s President Jonathan Sign the Cybercrime Bill Into Law.”

\textsuperscript{49} Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, Section 38.

\textsuperscript{50} According to Section 38(4): “Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction” (emphasis added). Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, \url{http://bit.ly/1LmHh7h}.
The 2013 “Guidelines for the Provision of Internet Service” published by the NCC also require ISPs to cooperate with law enforcement and regulatory agencies in providing “any service-related information... including information regarding particular users and the content of their communications” during investigations of cybercrime or other illegal activity.51 No details are provided in the guidelines regarding the oversight mechanisms required to prevent government authorities from acquiring free access to user information. The guidelines also stipulate that ISPs must retain user data and “the content of user messages or routing data” for at least 12 months.52

SIM card registration requirements instituted in June 2009 threaten users’ rights to anonymous communication and privacy,53 particularly in the absence of a data protection law.54 Anonymity is also compromised by user registration requirements in cybercafes under the new Cybercrime Law passed in May 2015. Under Section 7 of the law, cybercafes must make their registers “available to law enforcement personnel whenever needed,” with no clear measures for judicial oversight.55 This provision follows an October 2013 directive from the regulator that requires cybercafes to register customers and “maintain an up-to-date database of subscribers and users, including their full names, physical addresses, passport photos, and telephone numbers,” as part of the government’s efforts to combat cybercrime.56 The regulator was proactive in enforcing these requirements in 2014, finding 128 illegal cybercafes operating in Kano state without a license.57

Intimidation and Violence

Compared to print and broadcast journalists, online journalists and internet users have not been subject to significant extralegal intimidation or threats for their activities. The Nigerian authorities have a history of harassing and arresting traditional media workers, who faced greater restrictions and attacks by security forces and militant groups in the lead up to the March 2015 elections.58 The precarious environment for Nigerian journalists is exacerbated by a culture of impunity for crimes against media workers.59

Online users are occasionally harassed by the authorities for their online activities. On May 5, 2014, the State Security Service visited the office of a prominent digital media freedom activist, ‘Gbenga Sesan, after he had tweeted that citizens should hijack the hashtag for the 2014 World Economic Forum on Africa (#WEFAfrica) hosted in Nigeria to draw attention to the kidnapped Chibok girls and the #BringBackOurGirls campaign.60 The authorities summoned and questioned Sesan for a few hours before releasing him in an effort that stemmed from concerns that Sesan was embarrassing the country with his tweets.61

52 “Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission,” 3.
55 Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, Section 7.
58 Nkanga, “In election year, Nigeria’s press feeling the pressure.”
Nigeria

Technical Attacks

Cyberattacks are common in Nigeria, though most attacks are against government websites and carried out by the Naija Cyber Hacktivists, a group that has claimed responsibility for almost all cyberattacks to date. During the 2015 presidential elections, a new group calling itself the Nigerian Cyber Army hacked the website of the Independent National Electoral Commission (INEC), claiming that it did so to ensure free and fair elections. One distributed denial of service (DDoS) attack against the independent news outlet Premium Times was reported during its presidential election coverage.

Pakistan

Key Developments: June 2014 – May 2015

• In March 2015, Prime Minister Nawaz Sharif disbanded an inter-ministerial committee responsible for censorship and authorized the government regulator to undertake content management (see Blocking and Filtering).

• In November 2014, police in Lahore arrested a man who had evaded blasphemy charges related to his blog for three years (see Prosecutions and Detentions for Online Activities).

• In January 2015, the National Assembly introduced the draft Prevention of Electronic Crimes Bill, including overbroad definitions of criminal activity online (see Legal Environment).

• In August 2014, two journalists and an accountant were shot dead by unidentified gunmen in their offices of the Online International News Network in Balochistan (see Intimidation and Violence).
Pakistan

Introduction

Pakistan saw a democratic change of power in May 2013, when citizens voted the social democratic Pakistan People's Party (PPP) out of office, in favor of the conservative Pakistan Muslim League–Nawaz (PML-N) party under Prime Minister Nawaz Sharif. The government became the latest in a line of military and civilian authorities to restrict information and communication technologies (ICTs). Human rights monitors accused them of bolstering military and police powers, instead of addressing past abuses.

Though framed as necessary to combat terrorism and preserve Islam, censorship in Pakistan continues to reflect political motives, the influence of religious extremists, or a combination of the two. The video-sharing platform YouTube has been completely blocked in Pakistan since September 2012, when an anti-Islamic video sparked unrest around the Muslim world. Before the election, opposition politician Anusha Rehman criticized the ban, but has yet to lift it since her appointment as IT minister. Challenged in two high courts and the subject of persistent protests, this far-reaching ban continues to affect ordinary internet users, small businesses, and students, though many used digital tools to circumvent it or migrated to other online video services.

Other efforts could cement government control of Pakistan’s internet. Civil society groups said a pending cybercrime bill drafted with inadequate civil society consultation would disproportionately criminalize some online activities. In 2015, the government regulator was authorized to undertake censorship decisions previously handled by a nontransparent inter-ministerial committee, a change which lacks a legal foundation.

Obstacles to Access

Internet penetration is limited in Pakistan by a lack of resources, but mobile internet access is increasing with the recent launch of faster 3G and 4G service. However, Pakistani authorities frequently disable mobile internet access during times of perceived political or religious sensitivity.

Availability and Ease of Access

Internet penetration in Pakistan stood at 14 percent by early 2014, according to the International Telecommunication Union. A mobile survey company calculated the figure at 16 percent, half of which was through mobile phones. Pakistan’s telecommunications regulator reported mobile penetration at 73 percent. Internet penetration is expected to increase with the recent launch of 3G and 4G technology (see ICT Market).

Low literacy, difficult economic conditions, and cultural resistance have limited the proliferation of

---

ICTs in Pakistan. While the cost of internet use has fallen considerably in the last few years, with prices around US$12 a month for a broadband package in 2015, access remains out of reach for the majority of people in Pakistan.

Though ICT usage by girls and women in Pakistan is gradually increasing, online harassment unfortunately discourages greater utilization of ICTs by women, especially those under 30.

Most remote areas lack broadband, and a large number of users depend on slow dial-up connections or EDGE, an early mobile internet technology. In such areas, meaningful online activity like multimedia training can be challenging.

Restrictions on Connectivity

The PTCL owns the country’s largest internet exchange point, Pakistan Internet Exchange (PIE), which has three main nodes—in Karachi, Islamabad, and Lahore—and 42 smaller nodes nationwide. PIE operated the nation’s sole internet backbone until 2009, when additional bandwidth was offered by TransWorld Associates on its private fiber-optic cable, TW1. PTCL also controls access to the three international undersea fiber-optic cables: SEA-ME-WE 3 and SEA-ME-WE 4 connects Southeast Asia, the Middle East, and Western Europe; and I-ME-WE links India, the Middle East and Western Europe. The company signed an agreement to build the fourth one, considered to be one of the world’s largest, in 2014. The AAE-1 cable, projected to be completed by 2016, will connect countries in Asia, Africa, and Europe.

Damage to these cables did not cause access disruptions during the coverage period, as it had done in past years, but connectivity was still subject to physical interruption. In early 2015, villages in the northern Drosh Valley faced internet and telephone disconnection because of damage to the open main cable.

Several parts of western areas of Pakistan lack internet access, partly because of underdevelopment and partly because of ongoing conflicts. More than 75 percent of tribal areas and 60 percent of Balochistan province didn’t have fiber optic cables as of 2013.

As in previous years, Pakistan overall faced electricity shortages in 2014, especially when demand peaks during the summer months. Besides the usual load shedding and rolling blackouts, in 2014 and 2015, much of the country was also plunged into darkness at least four times when the national electricity grid collapsed due to rise in demand or explosion at one of the sites.

---

Pakistan

Security considerations continued to intrude on telecommunication services. In 2014 and 2015, as in previous years, the government suspended cellular services on some religious holidays in what the government termed “sensitive places.”¹³ The services, it is said, can be misused to undertake terrorist acts, but shutting them down limits access for the wider population.

ICT Market

The internet service providers (ISPs) association listed 50 operational ISPs in Pakistan in 2014, 10 of which provide DSL services.¹⁴ The government regulator, the Pakistan Telecommunication Authority (PTA), exerts significant control over internet and mobile providers through a bureaucratic process that includes hefty licensing fees.¹⁵ Broadband subscriptions, based on DSL—which uses existing telephone networks—or wireless WiMax technology, are concentrated in urban areas. The predominantly-state-owned Pakistan Telecommunication Company Limited (PTCL) controls 60 percent of the broadband market.¹⁶ An inquiry report found that other DSL operators cannot compete with PTCL, due to which some were forced to quit. PTCL denies these charges.¹⁷

After several years delay, Pakistan finally introduced internet-capable 3G mobile network and 4G spectrum, in April 2014. The 3G bid was won by four foreign-owned companies namely Mobilink, Zong, Telenor, and Ufone, whereas the 4G spectrum was won by Zong. In this bidding exercise, Pakistan secured US$903 million from 3G mobile network and US$210 million from 4G spectrum auctions, respectively. These networks will provide faster internet services to consumers in Pakistan.¹⁸ Although these services are so far limited to urban centres, mobile companies claim to be rapidly expanding the networks, with one company claiming to launch the 3G network in 32 cities.¹⁹ Since the launch of these services, their subscriber bases have been increasing, with over 9 million subscribers by the end of January 2015.²⁰

Mobile operators such as Mobilink, Ufone, Telenor, Warid, and Zong still struggle to attract customers due to high prices and poor coverage. Wireless service providers using the high-capacity data network WiMAX or high-speed broadband technology EVDO are also considered expensive.

Internet cafes do not require a license to operate, and opening one is relatively easy.²¹ Some child rights groups argue that cafes should be regulated to prevent inappropriate access to pornography and gambling sites.²²

¹⁶ Adam Senft, et al., O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Net sweeper’s Role in Pakistan’s Censorship Regime, Citizen Lab, June 20, 2013, https://citizenlab.org/2013/06/o-pakistan/.
Pakistan

Regulatory Bodies

The PTA is the regulatory body for the internet and mobile industry, and international free expression groups and experts have serious reservations about its openness and independence.\(^{23}\) The prime minister appoints the chair and members of the three-person authority, which reports to the Ministry of Information Technology and Telecommunication.\(^{24}\) The repeated failure to make these appointments in the past year further undermined the PTA’s reputation. In March 2015, the PTA formally took responsibility for internet content management (see Blocking and Filtering).

Limits on Content

In March 2015, Prime Minister Sharif disbanded the committee responsible for censorship decisions and authorized the PTA to undertake content management. Though the step was taken in part due to a petition questioning the committee’s authority, the regulator also lacks the necessary legal backing to undertake censorship. YouTube remains blocked, but other platforms, media, and communication tools are popular and contribute to a vibrant online space.

Blocking and Filtering

“Internet content management” lacks an adequate legislative framework. A range of overbroad provisions in the 1996 Pakistan Telecommunications Act supports censorship for the protection of national security or religious reasons.\(^{25}\) Authorities also cite Section 99 of the penal code, which allows the government to restrict information that might be prejudicial to the national interest, to justify filtering antimilitary, blasphemous, or anti-state content.\(^{26}\) Critics believe these issues can serve as cover for politically motivated censorship of dissenting voices. Information perceived as damaging to the image of the military or top politicians, for example, is also targeted.

In past years, the task of ordering blocks was undertaken by the Inter-Ministerial Committee for the Evaluation of Web Sites (IMCEW), comprised of representatives from PTA and the government, along with “men from the Ministry of Religious Affairs, the Inter-Services Intelligence, and Military Intelligence.”\(^{27}\) In December 2014, however, the Islamabad High Court restrained the Committee from blocking websites until any conclusion on its role is reached, following a petition challenging IMCEW’s authority.\(^{28}\)

In February 2015, the Ministry of Information asked the government to empower a new cell within the government regulator, the Pakistani Telecommunication Authority (PTA), to censor online content.\(^{29}\) Because the PTA is not legally authorized to block content, either the PTA Act would have

---

25 Article 19, “Pakistan: Telecommunications (Re-organization) Act.”
Pakistan

to be amended or executive directives would have to be issued to authorize the new function.\textsuperscript{30} In March 2015, Prime Minister Sharif complied, disbanding the Inter-Ministerial Committee and authorizing the PTA to undertake content management.\textsuperscript{31}

Historically, blocking orders have directed ISPs and backbone providers to implement manual blocks on individual URLs or IP addresses, their compliance ensured by licensing conditions.\textsuperscript{32} Since 2012, successive administrations have sought to introduce technical filtering.\textsuperscript{33} The National ICT Research and Development Fund initially requested that companies develop nationwide blocking technology to ”handle a block list of up to 50 million URLs,”\textsuperscript{34} though the status of that project was left in doubt after widespread civil society protests.\textsuperscript{35} News reports in 2013 and 2014 said PTA and government officials were still pursuing filtering solutions.\textsuperscript{36}

However, in 2013, the University of Toronto-based research group Citizen Lab reported that technology developed by the Canadian company Netsweeper was already filtering political and social content at the national level on the PTCL network.\textsuperscript{37} ”In addition to using Netsweeper technology to block websites, ISPs also use other less-transparent methods, such as DNS tampering,” Citizen Lab noted.\textsuperscript{38} The report highlighted the lack of transparency and accountability surrounding censorship in Pakistan, as tactics become more advanced.

The same lack of transparency extends to the content affected by censorship, which is often inconsistent based on location or across ISPs.\textsuperscript{39} There are no published guidelines outlining why content is blocked or how to appeal. Individuals and groups can also initiate censorship by petitioning courts to enact moral bans on online or traditional media content.\textsuperscript{40}

Censorship targeting pornography can affect access to legitimate content like Scarleteen, a U.S.-based sex education website for teenagers.\textsuperscript{41} Some users found Google Scholar search results for terms like breast anatomy or breast cancer also appeared to be blocked on the PTCL network in 2014.

\textsuperscript{30} Haider, ”PTA may be empowered.”
\textsuperscript{32} PTA Act 1996, art. 23.
\textsuperscript{33} Danny O’Brien, ”Pakistan’s Excessive Internet Censorship Plans,” Committee to Protect Journalists (blog), March 1, 2012, \url{https://cpj.org/x/4995}.
\textsuperscript{37} Senft, et al., O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Net sweeper’s Role in Pakistan’s Censorship Regime.
\textsuperscript{38} DNS tampering intercepts the user’s request to visit a functioning website and returns an error message.
\textsuperscript{39} OpenNet Initiative, ”Country Profile—Pakistan,” 2012.
\textsuperscript{40} ”Internet censorship: Court asked to ban inappropriate content,” The Express Tribune, June 14, 2011, \url{http://bit.ly/OCZFP}.
\textsuperscript{41} ”Pakistan blocks access to teen sex-ed site,” The Express Tribune, March 20, 2012, \url{http://bit.ly/1QeDDpE}.
Pakistan

Blocking frequently targets social media and communication apps. Since 2012, the government has blocked YouTube in response to the anti-Islamic video “The Innocence of Muslims.” The site was briefly unblocked in December 2012 until a broadcast journalist demonstrated that the offensive clip was still available.

Civil society groups protested against the ban, and in 2013, petitioners challenged it in the high courts in Lahore and Peshawar. Hearings in both cases are ongoing. Government officials encouraged Google to establish a version of YouTube in Pakistan’s jurisdiction, where it would be subject to government content management. News reports said Google, which owns the platform, declined to establish a local office because of the lack of intermediary liability protection for content providers under Pakistani law. In 2015, the Minister of Information told the Senate that the government is in the process of “providing Intermediary Liability Protection for internet content providers through Prevention of Electronic Crime Bill 2014”. However, details of the protection and its ultimate impact on the availability of YouTube remain unclear.

Political dissent and secessionist movements in areas including Baluchistan and Sindh province, where a Sindhi nationalist movement advocates for political divisions along ethnic lines, is among the nation’s most systematically censored content. In November 2013, the PTA requested that ISPs block the international website IMDb (Internet Movie Database), an order they reversed after two days. Analysts said the apparent ban—which attracted widespread criticism on social media—was related to the upcoming release of a British short film, “The Line of Freedom,” a fictional depiction of Pakistani security agencies abducting Baloch separatists. In 2014, IMDb was largely accessible again, yet the page documenting “The Line of Freedom” was still blocked. Pages relating to the movie are also inaccessible on other sites.

Authorities also target users seeking to access blocked content. In 2011, the PTA sent a legal notice to all ISPs in the country urging them to report customers using encryption and virtual private networks (VPNs)—technology that allows internet users to interact online undetected and access blocked websites—to curb communication between terrorists. International and civil society organizations in Pakistan protested, and the tools remain widely used to access YouTube. Two of the

---

45 Jajja, “YouTube Ban: Google to appear before Lahore High Court.”
Pakistan

best-known services, Spotflux and HotSpot VPN, became inaccessible in January 2014, and Spotflux said the government had actively blocked its services.55 Both were later restored.

Content Removal

Extralegal pressure on publishers and content producers by the state or other actors to remove content is not unknown in Pakistan, but frequently goes unreported. Takedowns by international companies are more high profile. Facebook and Twitter are among the companies publicly criticized for limiting access to content at the government’s request, “under local laws prohibiting blasphemy and criticism of the state.”56 Both reversed some such decisions and republished content they had previously restricted in mid-2014.57

Official requests to remove content also lack transparency. Following a major terrorist attack in December, the government ordered material published by banned terrorist outfits to be removed from the internet, though published reports did not elaborate on the process involved.58

Media, Diversity, and Content Manipulation

Despite existing limitations on online content—and looming new ones—Pakistanis have relatively open access to international news organizations and other independent media, as well as a range of websites representing Pakistani political parties, local civil society groups, and international human rights organizations.59 ICTs, particularly mobile phones, promote social mobilization. Most of social networking, blogging, and VoIP applications were available and widely used during the coverage period. Nevertheless, most online commentators exercise a degree of self-censorship when writing on topics such as religion, blasphemy, separatist movements, and women’s and LGBTI rights.

Digital Activism

Human rights activists have also been able to galvanize public support against militancy through new technology. One such incident occurred in December 2014, when an influential cleric in Islamabad refused to categorically condemn a terrorist attack on a school. Human rights activists gathered outside the cleric’s mosque, demanding an apology for the previous statement.60 The call to protest originated through social media and text messages using the #ReclaimYourMosque hashtag.61 Meanwhile, a Taliban spokesman called the protest organizer, threatening him to back off or “be ready for consequences.”62

Violations of User Rights

Violations of user rights continued at high levels during the coverage period, including fatal attacks on an online newsroom and at least one arrest in relation to allegations of blasphemy online. Problematic laws were also under debate, including a law to combat cybercrime, which civil society groups say could criminalize online activity—though their involvement in the drafting process has been hampered by officials. Researchers uncovered compelling information about Pakistani agencies’ surveillance ambitions and capabilities during the coverage period.

Legal Environment

Article 19 of the Pakistani constitution establishes freedom of speech as a fundamental right, although it is subject to several restrictions. Pakistan became a signatory to the International Covenant on Civil and Political Rights in 2010.

Existing laws also have the potential to restrict internet users. The 2004 Defamation Act allows for imprisonment of up to five years, and observers fear a chilling effect if it is used to launch court cases for online expression. Section 124 of the penal code on sedition “by words” or “visible representation” is broadly worded, though it has yet to be applied in an online context.

Section 295(c) of the penal code, which covers blasphemy, is frequently invoked to limit freedom of expression. Any citizen can file a blasphemy complaint against any other, and human rights groups say charges have been abused in the past to settle personal vendettas. The imputation of blasphemy leaves the accused vulnerable to reprisals, regardless of whether it has foundation. Some cases of reprisals have involved electronic media.

Several laws to try terrorism can also been exploited against internet users. The Pakistan Protection Act, supposedly a reformulation of a problematic Pakistan Protection Ordinance in effect during the previous coverage period, passed in July 2014. Though it included some amendments, critics said it failed to address concerns expressed by lawyers and civil society groups, who said language criminalizing unspecified cybercrimes as acts of terror was vague and open to abuse.

Taking note of the absence of law to deal with cybercrime, the relevant authorities have pushed for passing an anti-cybercrime law. A draft Prevention of Electronics Crimes Act 2015, though it contains some procedural safeguards for cybercrime investigation by law enforcement agencies, could grant intelligence agencies unrestricted mass surveillance powers. Critics said it lacked clear definitions, while criminalizing some specific activity like “defamation of women.” Civil society groups recommended its amendment in accordance with international standards.

---

67 This data includes the “communication’s origin, destination, route, time, data, size, duration or type of underlying service.”
Pakistan

On May 25, 2015, the National Standing Committee on Information Technology and Telecommunication held a hearing to discuss the bill. Though it was characterized as a public hearing, only seven civil society stakeholders were invited, and two of those were uninvited at the last minute. Despite this miscommunication, the standing committee listened to critics and asked its members to hold consultations with experts to revise the bill, which was approved by the IT standing committee in September, though some committee members said they had not read the approved draft, and no major changes were incorporated as a result of the consultation. The national assembly must approve the bill before it becomes law.  

The Surveying and Mapping Act, 2014, first introduced in 2012, limits digital mapping activity to organizations registered with the governmental authority Survey of Pakistan, with federal permission required for mapping collaboration with foreign companies. The Senate approved the Act in June 2014. 

Prosecutions and Detentions for Online Activities

New blasphemy accusations declined from the previous coverage period, but cases from the past continued to haunt the accused. In November 2014, in Chakwal, a Christian accused of blaspheming online, was arrested in Lahore. The man, who used to write on his personal blog, went into hiding three years ago when he was first accused.

Even high profile individuals came under increased scrutiny on the internet. In January 2015, a pop-star turned Islamic evangelist faced blasphemy accusations when his video making controversial remarks went viral online. The evangelist later filmed an apology, but mounting pressure forced him to leave for the United Kingdom. Separately, a private TV channel owner, host, and guests were charged with blasphemy in relation to a video from a morning show, which went viral online after its allegedly offensive content was publicized by a rival channel.

Surveillance, Privacy, and Anonymity

Government surveillance is a concern for activists, bloggers, and media representatives, as well as ordinary internet users. Pakistani authorities, particularly intelligence agencies, appear to have been expanding their monitoring activities in recent years, while provincial officials have been exerting pressure on the central government to grant local police forces greater surveillance powers and location tracking abilities, ostensibly to curb terrorism and violent crimes.
Pakistan

Details of these activities were documented by researchers in the past two years. In 2015, an investigation by U.K.-based Privacy International revealed that the practical surveillance capability of the Pakistani government, particularly the Inter-Services Intelligence Agency, now outstrips domestic and international law regulating that surveillance. "Mass network surveillance has been in place in Pakistan since at least 2005," using technology obtained "from both domestic and foreign surveillance companies, including Alcatel, Ericsson, Huawei, SS8 and Utimaco," according to the report.

In 2013, a report by Citizen Lab indicated that Pakistani citizens may be vulnerable to oversight through a software tool present in the country. FinFisher’s "Governmental IT Intrusion and Remote Monitoring Solutions" package includes the FinSpy tool, which attacks the victim’s machine with malware to collect data including Skype audio, key logs, and screenshots. The analysis found FinFisher's command and control servers in 36 countries globally, including on the PTCL network in Pakistan. This did not confirm that actors in Pakistan are knowingly taking advantage of its capabilities. In 2014, however, hackers released internal FinFisher documents indicating that a client identified as "Customer 32" licensed software from FinFisher to infect Microsoft office documents with malware to steal files from target computers in Pakistan.

In 2015, in a separate hacking attack, internal documents were stolen from the Italy-based surveillance software company Hacking Team, and released online. Analysis of the company’s interactions with individuals in Pakistan revealed they had been in touch with private sector representatives “for years,” and that police sought equipment that would work on older models of cellphone common in Pakistan, among other details.

The Fair Trial Act, passed in 2013, allows security agencies to seek a judicial warrant to monitor private communications “to neutralize and prevent [a] threat or any attempt to carry out scheduled offences.” It covers information sent from or received in Pakistan, or between Pakistani citizens whether they are resident in the country or not. Critics say that the act’s wording leaves it open to abuse, though none has been publicly reported. Under the law, service providers face a one-year jail term or a fine of up to PKR 10 million (US$103,000) for failing to cooperate with warrants. While the requirement for a warrant is positive, one can be issued if a law enforcement official has "reason to believe" in a terrorism risk; it can also be temporarily waived by intelligence agencies. Digital Rights Group issued a white paper, analyzing the provisions of the Fair Trial Act contradictory to the Constitution and contrary to the International Treaties Pakistan has signed in the past.

ISPs, telecommunications companies, and SIM card vendors are required to authenticate the Computerized National Identity Card details of prospective customers with the National Database Regis-

Pakistan

A registration drive was launched following a December 2014 attack on a school that killed more than 150 students. Investigators tracked three unregistered SIM cards used by the terrorists for communication during the attack. Following the attack, the government began a crackdown on "unregistered" SIM cards; asked citizens to verify numbers registered against their names; and finally, mandated all mobile customers to register their mobile numbers against their biometric thumb impression. In early 2015, the government launched a fresh SIM card registration drive, making biometric verification mandatory. Those SIM cards that did not register biometric identification protocols were warned of automatic disconnection, though the PTA chairman admitted the system was not foolproof.

A 2007 Prevention of Electronic Crimes Ordinance requiring telecommunications companies to retain user traffic data for a minimum of 90 days, and share logs of customer communications with security agencies when directed by the PTA, expired in 2009, though the practices reportedly continued.

Intimidation and Violence

Pakistan is one of the world’s most dangerous countries for traditional journalists. Violence has yet to affect online journalists in the same way, though they can also be vulnerable. In August 2014, two journalists and a network accountant were shot dead by unidentified gunmen in their offices of the Online International News Network in Balochistan.

Violence against women thought to have brought shame on their communities—including honor killings—has begun to involve ICT usage. In one high-profile case from 2012, the Pakistani Taliban claimed responsibility for shooting 15-year-old Malala Yousufzai in the head while she was traveling in a school van in the Swat region, partly in retaliation for blogging. She survived and was awarded the Nobel Peace Prize in 2014.

Leaking explicit photos, threats of blackmail, and other incidences of online harassment are increasing in Pakistan. More than three thousand cybercrimes were reported to the Federal Investigation Agency from August 2014 to August 2015. Of those cases, 45 percent targeted women on social media. The figures only represent reported cases—many victims do not come forward for fear of losing access to ICTs. No data has been provided for other provinces.

In June 2014, a local judge in Lahore asked the Federal Investigation Agency to probe whether a

---

Pakistan

Facebook page had been posting blasphemous content online.91 A month later, in Gujranwala, a mob burned five houses of Ahmadis, killing three Ahmedi women and injuring eight others who were accused of sharing blasphemous post on Facebook.92

Militant Islamic groups have launched attacks on cybercafes and mobile phone stores in the past for allegedly encouraging moral degradation.93 No attacks were documented during the coverage period of this report.94

Free expression activists and bloggers have also reported receiving death threats. Many publicize the threats—and sometimes attract more—on Twitter. Most are sent via text message from untraceable, unregistered mobile phone connections, often originating from the tribal areas of the country, and several include specific details from the recipient’s social media profiles or other online activity.

Technical Attacks

Technical attacks against the websites of nongovernmental organizations, opposition groups, and activists are common in Pakistan but typically go unreported due to self-censorship. The websites of government agencies are also commonly attacked, often by ideological hackers attempting to make a political statement.95 In 2015, the website of the religious political party Jamaat-e-Islami was hacked for its alleged support of terrorists.96

Officials allege that most cyberattacks originate in India; on the other hand, many Pakistanis also hack Indian websites.97

A center in the FIA known as the National Response Centre for Cyber Crimes (NR3C) is supposed to deal with cyber criminals involved in electronic theft, forgery, and other crimes. According to sources in NR3C, there has been 30 percent rise in complaints related to cybercrime.98 Yet, critics say the FIA’s actions are not uniform, and that attacks affecting regular internet users are frequently ignored. The FIA has responded that due to the absence of a law defining cybercrime, the body is unable to ensure that all criminals will be brought to justice.99

94 Two men died in a shooting attack on an internet café in Karachi which was later reported to be targeting a specific customer, not the venue. “Two killed in attack on internet café,” Dawn, November 1, 2013, http://bit.ly/1NyPdZq.
98 Sher, “Absence of comprehensive law against cybercrimes: NR3C of FIA unable to take action against criminals.”
Philippines

### Internet Freedom Status

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>27</td>
<td>27</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

### Key Developments: June 2014 – May 2015

- In an unprecedented move, the government ordered telecommunication companies to block mobile signals in the capital region during a papal visit, temporarily depriving approximately 20 million subscribers of access (see Restrictions on Connectivity).
- In October 2014, a senator filed criminal libel charges against a journalist in relation to allegations of corruption published on a personal blog (see Prosecutions and Detentions for Online Activities).
- Police are investigating the targeted assassination of a former journalist in April 2015 for a possible connection to her online comments on social and political issues (see Intimidation and Violence).
Philippines

Introduction

Internet freedom in the Philippines has been gradually declining since the country was first evaluated in 2012. Although still categorized as “free,” little progress has been observed in terms of improving access to the internet, limited by high subscription costs and service that barely reaches the population outside major cities. Access was undermined when authorities restricted network coverage during the papal visit in 2015.

Libel cases accounted for 16 percent of “cybercrime” incidents documented by police in 2014, in the wake of the Supreme Court’s 2014 ruling stating that online libel is a crime under the Cybercrime Prevention Act of 2012. Countermeasures to this law, the Magna Carta for Internet Freedom and the Crowdsourcing Act of 2013, were stalled in the legislature during the coverage period of this report. On a positive note, the Senate approved a Freedom of Information bill in 2014, with its counterpart in the lower chamber awaiting second reading.

Protection of journalists working in the country has not improved, although online journalists have yet to experience the same level of violence as mainstream journalists. The killing of outspoken internet user Melinda Magsino on April 13, in a targeted shooting reminiscent of the frequent attacks on radio commentators and other media practitioners in the Philippines, caused concern that this situation may be changing for the worse, though police and press freedom groups are still investigating to establish whether her murder was related to her online activities.

Obstacles to Access

Mobile phone subscribers experienced widespread blocking of network coverage in the capital region during the visit of the Catholic Church leader Pope Francis. For almost five days in January, service providers blocked network coverage for almost 20 million people living in the Manila metropolitan area on the direct order of the president through the National Telecommunications Commission. In a significant step to boost internet speed and affordability in the country, both houses of Congress initiated an inquiry into the poor performance of broadband amid high subscription rates, following a study by a private firm listing the Philippines as having the worst internet service in Southeast Asia.

Availability and Ease of Access

Internet penetration increased to 40 percent by 2014, up from 37 percent in 2013.¹ Connectivity is concentrated mainly in urban areas, while rural areas remain largely underserved.² To address this divide, the government announced that it would be providing free Wi-Fi service to some 600 municipalities in remote areas through TV White Space technologies with the help of telcos in 2015.³ Dubbed “Super Wi-Fi,” this method of tapping unused TV channels for wireless data delivery was first introduced in the Philippines in 2013 to serve fishermen in the Visayas region.⁴

---

Mobile phone subscriptions have increased significantly in recent years, with penetration reaching 111 percent in 2014, indicating that some users have more than one device.\(^5\) By the third quarter of 2014, leading telcos Philippine Long Distance Telephone Co. (PLDT) and Globe Telecommunications reported a combined 110 million mobile phone subscribers,\(^6\) in a country with a population of 100 million.\(^7\) Despite this, there were only 3.1 million mobile broadband subscribers by late 2014,\(^8\) following the deployment of 4G LTE and HSPA+ technologies in the previous year,\(^9\) slightly better than the 2.5 million subscribing to fixed broadband.\(^10\)

The slow uptake of broadband internet in the country, and the consequently low internet penetration, is largely due to steep subscription fees. The cost and slow speed of internet service was a prominent issue in the past year, with a couple of lawmakers initiating inquiries into steep charges and poor performance;\(^11\) telcos being summoned by the government to discuss minimum broadband speed – a move firmly rejected by telcos in a position paper;\(^13\) and the PLDT publicly blaming “abusive” internet users for the slow speeds.\(^14\) Akamai reported the average connection speed in the country at 2.5 Mbps in the third quarter of 2014, no change from the previous year.\(^15\) Not only does the Philippines have the slowest internet speed in the region, it also has the most expensive subscriptions.\(^16\) In early 2015, PLDT was charging a minimum monthly subscription fee for fixed broadband at US$29 for up to 2Mbps, a significant increase from last year’s $22; while Globe’s charges remained at $24.\(^17\)

### Restrictions on Connectivity

In a departure from previous years, the government ordered a sporadic regional suspension of cellular services during the visit of Pope Francis from January 15 to 19, 2015.\(^18\) Telcos sent text messages to mobile phone subscribers announcing service interruption, citing a directive from the National Telecommunications Commission to block network coverage in areas visited by the Pope for security reasons.\(^19\) The government stated concerns over the potential for remote detonation of explosives via mobile phone, a justification criticized by at least one lawmaker.\(^20\)

According to latest government data from 2012, the Philippines has 360 operating ISPs.\(^21\) Many

---

6 Quarterly reports to the Securities and Exchange Commission (SEC), as of September 30, 2014.
8 Quarterly reports to the SEC, as of September 30, 2014.
of these connect to PLDT, which owns the majority of fixed-line connections as well as the 10,000 kilometer domestic fiber-optic network that connects to several international networks. Since the completion of a new cable linking the central provinces of Palawan and Iloilo in January 2014, the company now owns or partly owns five out of nine international cable landings.

ICT Market

Companies entering the market go through a two-stage process. First, they must obtain a congressional license that involves parliamentary hearings and the approval of both the upper and lower houses. Second, they need to apply for certification from the National Telecommunications Commission. The constitution limits foreign ownership of local businesses to 40 percent. Internet service is currently classified as a value-added service and is therefore subject to fewer regulatory requirements than mobile and fixed phone services.

In the 1990s, government legislation allowed competitors a foothold in a market previously dominated by the PLDT, a company that had been U.S.-owned and Philippine government-owned before its current incarnation as a private entity. However, in the absence of antitrust laws to promote healthy competition between businesses, the PLDT now controls 70 percent of the country's ICT sector.

House Bill 5286, or the Philippine Fair Competition Act, a bill that would dismantle monopolies, has been languishing in the House of Representatives for at least 23 years since it was filed in the 8th Congress (1987-1992).

Globe is the sole challenger to PLDT, after it purchased debts from struggling competitor Bayan Telecommunications in early 2013. The complete takeover of Bayantel by Globe has been heavily contested by PLDT, alleging that the move would result into a disproportionate distribution of frequencies, on grounds that Globe would have significantly more frequencies per subscriber than PLDT.

Regulatory Bodies

The National Telecommunications Commission has regulated the industry with quasi-judicial powers and developed tariff and technical regulations, licensing conditions, and competition and interconnection requirements since its creation in 1979.

In 2015, business groups urged the Senate to act on the still pending Senate Bill No. 50 to create a specialized Department of Information and Communications Technology, citing the need to boost the country's competitiveness through a streamlining of ICT-related agencies. The bill has been

---

pending before a bicameral conference committee since March 2012. Three years later, on March 11, 2015, some members of the 16th Congress reintroduced the bill as Senate Bill No. 2686 and was approved during the third reading on June 1. It has been with the lower chamber awaiting concurrence since June 4.  

At present, institutions governing the ICT sector are highly bureaucratic, often with ambiguous or overlapping responsibilities that slow the pace of development. Successive government administrations—including that of President Benigno Aquino—have modified the structure of official ICT bodies. His Executive Order 47 of 2011 established an Information and Communications Technology Office (ICTO) under the Department of Science and Technology (DOST) tasked with conducting research, development, and capacity-building in the ICT industry. However, the division of labor between this office and the Department of Transportation and Communications, which also deals with ICT-related communications, as well as the National Computer Center and the Telecommunications Office, is hard to perceive. If an ICT department is approved, all other ICT-related agencies will be abolished and their powers and personnel transferred to its jurisdiction.

All relevant government bodies are headed by presidential appointees. Critics believe this creates a dependence on the incumbent administration, which determines their budget.

**Limits on Content**

*Freedom of expression online was tested in the country after news of a deadly encounter between the national police and the Muslim insurgents made national headlines. A video of the actual killings went viral on YouTube and was shared multiple times on different social media platforms, which prompted the president to issue a takedown order and the National Bureau of Investigation to investigate the origin of the video as well as those sharing and liking it. Online activism was less prominent than in previous years, when activists organized street protests through online campaigning.*

**Blocking and Filtering**

No systematic government censorship of online content has been documented in the Philippines, and internet users enjoyed unrestricted access to both domestic and international sources of information during the coverage period of this report. Internet users freely access social networks and communication apps including YouTube, Facebook, Twitter, and international blog-hosting services. Although rare, blocking and filtering of content is allowed under a law that requires ISPs to prevent access to pornographic sites. The Department of Justice briefly sought to block Canada-based online dating site Ashley Madison after it launched in the country in November 2014. According to Department Secretary Leila De Lima, “The website is a platform that allows illegal acts to be eventually committed. A ban may be enforced,” referring to the website’s promotion of extramarital affairs, which are illegal.

---

33 The Revised Penal Code of the Philippines states that concubinage is a crime committed by “any husband who shall keep a mistress in the conjugal dwelling, or shall have sexual intercourse, under scandalous circumstances, with a woman who is not
Philippines

The justice department backtracked a month later, stating that it could only request that telcos and ISPs block the website, rather than mandate it. This followed the Supreme Court’s ruling earlier in the year against Section 19, the infamous “takedown” clause of the 2012 Cybercrime Prevention Act that would have allowed the Department of Justice to “restrict or block” overly broad categories of content without a court order. In February, however, the Supreme Court ruled the section unconstitutional, while upholding other provisions criminalizing online libel (see Legal Environment).

Content Removal

In early 2015, 44 members of the Philippine National Police Special Action Force in Mamasapano, Maguindanao, in the southern Philippines, were killed, allegedly by Muslim insurgents. Video of the Mamasapano Massacre, as it was dubbed in media reports, went viral on YouTube, eliciting public anger against the uploader of the video as well as the perpetrators, on grounds that sharing the footage was insensitive to the families. The Office of the President ordered the uploader to take down the video. After the individual refused to comply, the National Bureau of Investigation (NBI) threatened to go after the individual, and those who subsequently shared or “liked” it on social media. This announcement was issued in spite of the fact that the Supreme Court had found in their 2014 ruling against Section 5 of the Cybercrime law that it was unconstitutional to punish those who simply like or share a post or video online. The NBI later said they had identified the source of the video, but no criminal charges were reported.

On July 1, 2013, Senator Miriam Defensor Santiago refiled the Magna Carta for Philippine Internet Freedom in the Senate. The bill attracted widespread support and discussion on social media. Democracy.Net.PH, a group of internet freedom advocates, was particularly active, and Santiago credited the group for spearheading citizen participation in drafting a provision that “provides for court proceedings in cases where websites or networks are to be taken down and prohibits censorship of content without a court order.” The bill is pending in relevant committees and awaiting endorsement.

Media, Diversity, and Content Manipulation

Many news websites are online versions of traditional media, which self-censor due to the level of violence against journalists in the Philippines. While the same attitude may be reflected in their on-

Philippines

line output, the degree is difficult to establish. State officials and private authorities are periodically reported using harassment to suppress online speech.

More generally, the Philippine blogosphere is rich and thriving. Both state and nonstate actors actively use the internet as a platform to discuss politics, especially during elections. There have been no explicit government restrictions in place against any social media or communication applications in the Philippines.

Digital Activism

In the previous three years, digital activism in the country had a significant impact on addressing a number of contentious sociopolitical issues, making national and international headlines and prompting positive action from the government. Past successes include a 2013 protest against the alleged misuse of PHP 10 billion (US$220 million) from a Priority Development Assistance Fund, locally dubbed the “pork barrel,” by senators and members of congress. A Facebook petition called for the abolition of the fund and the filing of criminal charges against the lawmakers, and helped fuel nationwide protests. The Supreme Court subsequently declared the fund unconstitutional. In 2015, three senators and several NGO officials were in detention on charges of alleged corruption, while other lawmakers are still being investigated. In comparison, this coverage period saw a relatively low level of online participation in activist causes.

Violations of User Rights

The Philippines criminalized online libel in 2012, punishable by harsher penalties than offline libel, a rights violation that the Supreme Court failed to rectify when it considered the constitutionality of the law in 2014. During the coverage period, a senator filed a criminal lawsuit against a former aide who blogged about irregularities in the senator’s dealings with development projects. A former journalist who was active online was killed by armed men in broad daylight in April 2015, though whether it was in reprisal for digital activity remains unclear. On a positive note, the House of Representatives finally approved its counterpart Freedom of Information bill, 22 years after it was filed in Congress.

Legal Environment

The Bill of Rights of the 1987 constitution protects freedom of expression (Section 4) and privacy of communication (Section 1). However, some laws undermine those protections. Libel is punishable by fines and imprisonment under Articles 353 and 360 of the Revised Penal Code. This has historically been challenging to prove in online cases which lack a physical place of publication—one of the requirements for an offline prosecution—and in 2007, a Department of Justice resolution established that the Articles do not apply to statements posted on websites.

47 Department of Justice, Resolution No. 05-1-11895 on Malayan Insurance vs. Philip Piccio, et al., June 20, 2007. Article 353
Section 4c (4) of the 2012 cybercrime law, however, classified libel as a cybercrime. Section 6 stipulates a higher degree of punishment for online libel with imprisonment of up to eight years, almost double the maximum penalty for the identical offense perpetrated offline which is punishable by prison terms of six months to four years and two months under the revised penal code. The Supreme Court suspended implementation of the law after widespread protests, but in a February 2014 decision the court ruled that the libel provision was constitutional, keeping the disproportionate penalties on the books. However, it clarified that users reacting online to a libelous post—by “liking” it, for example—could not be held liable, and struck down Sections 12 and 19 that would have allowed law enforcers to monitor and collect real-time traffic data without a court order. On April 8, 2014, the Department of Justice began the first round of public consultations for the formulation of the Implementing Rules and Regulations (IRR) governing the act in accordance with Section 28, which gave the department 90 days to produce the IRR. After seven public consultations, the justice department concluded its review on June 11, 2015. This followed a Congressional inquiry into the three-year delay in the release of the IRR. Prior to the announcement, the justice department released guidelines on bail wherein PHP 10,000 (US$219) is required of anyone charged with online libel.

If passed, the Magna Carta for Internet Freedom would repeal the cybercrime law and treat online libel as a civil, not a criminal act, with penalties determined by the courts and commensurate to actual damages suffered. It also requires a court order for authorities seeking to obtain any data pertinent to acts it defines as criminal. It would further mandate the dissemination of public information as long as such information does not go against provisions in existing laws.

The Magna Carta initiative was supported by Senator Teofisto Guingona III, who separately filed the Crowdsourcing Act of 2013. Also known as Senate Bill No. 73, the act would not only allow citizens to participate in the legislative process through the use of ICTs, but also require lawmakers to include the people’s comments in committee reports concerning pending bills. If passed, it would make some important measures mandatory: People’s committee hearings to be held in Congress (Section 6); continuous online participation by citizens while debates are being held on the floor (Section 7); and a pre-approval consultation (Section 8) wherein the president of the Philippines must allow people to send online comments about a pending bill for five days, and subsequently

states that, “libel is committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means.” The Department also stated that the accused are not culpable because they cannot be considered as authors, editors, or publishers as provided for in Article 360. Critics have further noted that the Revised Penal Code, which dates from 1932, long predates digital technology, and therefore shouldn’t be applied to digital content.

Philippines

consider those comments for at least another three days, before signing a bill into law.\(^{58}\) Both bills were still pending in the Science and Technology Committee as of May 2015.

Twenty-two years after it was first filed in Congress, the Senate approved the People’s Freedom of Information Act of 2013 in March 2014.\(^{59}\) In November, the lower chamber also approved the bill, which critics said was watered down.\(^{60}\) The bill passed the Committee on Appropriations on March 4, 2015; the bill is awaiting second reading, the timeframe for which is not known.\(^{61}\)

Prosecutions and Detentions for Online Activities

At least one concerning libel case was filed during the coverage period in the wake of the Supreme Court’s ruling that punishing online libel under the Cybercrime Prevention Act is constitutional. On October 10, 2014, Senate President Franklin Drilon filed charges against a journalist who blogged about the senator’s alleged misuse of public funds.\(^{62}\) Charges are pending following the journalist’s posting bail on February 20, 2015.\(^{63}\) Earlier in 2014, Senator Drilon had publicly supported another senator’s proposal to decriminalize online libel.\(^{64}\)

In a report released on March 15, 2015, the justice department cited 614 cybercrime incidents recorded by the Philippine National Police Anti Cybercrime Group in 2014, an increase of more than 100 percent from the 288 cases in 2013. Libel accounted for 16 percent of cases in 2014, second only to internet fraud at 22 percent.\(^{65}\)

Surveillance, Privacy, and Anonymity

A 2012 Data Privacy Act established parameters for the collection of personal financial information and an independent privacy regulator.\(^{66}\) Other laws with privacy implications include the Anti-Child Pornography Act of 2009 which explicitly states that its section on ISPs may not be “construed to require an ISP to engage in the monitoring of any user,”\(^{67}\) though it does require them to “obtain” and “preserve” evidence of violations, and threatens to revoke their license for noncompliance; Section 12 of the law also authorizes local government units to monitor and regulate commercial establishments that provide internet services. Under the Human Security Act of 2007, law enforcement officials must obtain a court order to intercept communications or conduct surveillance activities.

Philippines

against individuals or organizations suspected of terrorist activity. To date, no abuse of this law has been reported.

There are no restrictions on anonymous communication in the Philippines. The government does not require user registration for internet and mobile access, and prepaid services are widely available, even in small neighborhood stores. However, reports about the increasing frequency of crimes committed on the internet, particularly rising incidents of child pornography, have prompted some government and law enforcement officials to call for a law requiring the registration of SIM cards for prepaid subscribers.

**Intimidation and Violence**

Violence against journalists is a significant problem in the Philippines. As of March 2015, the Committee to Protect Journalists reported at least 77 Philippine journalists had been killed in relation to their work—most covering political issues like corruption—since 1992. Not one of these murders has been fully prosecuted—meaning that not everyone responsible for ordering and executing each killing has been tried and convicted—creating an entrenched culture of impunity that sends the message that individuals exercising free speech can be attacked at will.

Fears that online journalists may experience the same violence were exacerbated early this year when two armed men shot and killed Melinda Magsino, a former broadsheet correspondent who later ran an online magazine, but who was no longer actively reporting. Some reports said she also wrote about current affairs on her personal Facebook page, but police were also investigating other possible motives.

In a case some observers described as harassment in response to online speech, university officials suspended a student for publicly protesting against increased school fees on Facebook in 2015.

**Technical Attacks**

There have been no reports of politically motivated incidents of technical violence or cyberattacks perpetrated by the government toward private individuals. However, as in the previous coverage period, hackers attacked several government websites. Responding to the Mamasapano massacre, the hacktivist group, Anonymous Philippines, claimed responsibility for altering government websites to display condolences for the families of the fallen Special Action Force unit, and criticism against President Aquino for mishandling the official response to the tragedy.
Russia

Key Developments: June 2014 – May 2015

- In June 2014, the president signed new amendments to the criminal code that increased penalties for disseminating materials online related to "extremism" or religious hatred, and criminalized the financing of extremist activity—a vague term that has been applied to the work of nongovernmental organizations and independent media outlets (see Legal Environment).

- The government continued to censor content related to the conflict in Ukraine and antigovernment protests, and threatened to block entire platforms due to the increasing difficulty of blocking individual pages (see Blocking and Filtering).

- In July 2014, the president signed a new data localization law that required technology companies processing Russians’ data to host the information on local servers. As companies decided how and whether to comply with the law ahead of the September 1, 2015, deadline, privacy advocates raised concerns that the rule could make Russians more susceptible to government surveillance (see Media, Diversity, and Content Manipulation and Surveillance, Privacy, and Anonymity).
Russia

Introduction

Internet freedom in Russia has deteriorated steadily over the past few years, with a steeper decline from 2013 to 2014 following the Euromaidan protests in neighboring Ukraine and Russia's subsequent annexation of Crimea. During this time, blocking of online content expanded significantly, and the government enacted a series of restrictive laws. Since mid-2014, the authorities have continued to constrict the environment for freedom of expression and information online by blocking or economically targeting critical media outlets, increasing criminal penalties for online activities, and prosecuting or arresting internet users for their posts.

In June 2014, the president signed new amendments to the criminal code that increased penalties for disseminating materials online related to "extremism," setting prison terms of up to five years, as well as increasing penalties for "inciting hatred" to terms of up to six years. Other amendments criminalized the financing of extremist activity—a vague phrase that has been applied to the work of nongovernmental organizations (NGOs) and independent media outlets. For example, the online news outlet Grani.ru, which had already suffered revenue losses after being blocked in March 2014 for allegedly extremist content, was unable to receive donations or funding due to these new amendments. In addition, in May 2015 a new law on "undesirable organizations" included bans on disseminating information from the blacklisted groups.

The government has continued to target social media and technology companies, though with varying success. Laws passed in May and July 2014 required the registration of bloggers and the storing of all Russians’ data on servers located within Russia, but they have been difficult to enforce. Nevertheless, many are concerned that data-localization rules could make it easier for the Russian government to access internet users’ information, infringing on their right to privacy. Meanwhile, the authorities continue to expand their capacity for surveillance of communications by requiring all internet and mobile service providers to upgrade to SORM-3 technology, which provides intelligence agencies with greater access to the content of communications through deep packet inspection (DPI).

Obstacles to Access

The internet penetration rate in Russia continues to grow, and the majority of would-be users can find internet access at an acceptable speed and for an affordable price. At the same time, the market for information and communication technologies (ICTs) is still heavily regulated, and most services are under direct or indirect state control.

Availability and Ease of Access

Internet access in Russia continues to expand. According to data from the Public Opinion Foundation, the internet penetration rate had reached 51 percent by the end of 2014, compared with 46 percent by the end of 2013.1 The International Telecommunication Union (ITU) places the figure somewhat higher, reporting an internet penetration rate of 71 percent by the end of 2014, compared

---

Russia

with 68 percent in 2013 and just 29 percent in 2009.\(^2\) More than half of internet users are under the age of 35. The speed of access is also increasing: According to Akamai, the average connection speed in Russia was 9 Mbps by the end of 2014, which is significantly higher than in most other post-Soviet states.\(^3\) In addition, the mobile phone penetration rate reached 155 percent in 2014,\(^4\) meaning there were more subscriptions than inhabitants; for mobile broadband subscriptions, the rate was 65.9 percent.\(^5\) According to a poll by the Russia Public Opinion Research Center, 55 percent of Russian internet users access the internet through smartphones, 73 percent with desktop computers, 33 percent with mobile phones, 41 percent via tablets, and 61 percent with laptops.\(^6\)

There is no significant gender divide when it comes to internet access in Russia.\(^7\) Nevertheless, there is variation in access among the regions, in terms of both speed and price. For instance, in Moscow and St. Petersburg, the average download speeds range from 16 to 19 Mbps, and the price of a monthly unlimited plan starts at US$6; in the rest of the country the average download speed is not more than 4 to 6 Mbps, while the minimum price in remote areas of the Far East is US$12 per month.\(^8\)

The median monthly income of Russian citizens in 2014, according to the Ministry of Labor and Social Protection, was US$680 (using the average annual conversion rate from the ruble).\(^9\) Therefore, the cost of internet access is about 1.3 percent of the average income, which indicates that access is relatively affordable. Indeed, according to figures cited by the authors of the study *Economics of the Russian Internet 2013–2014*, only 4 percent of Russians stated that they would like to use the internet but cannot afford it.\(^10\)

In May 2014, the Federal Communications Agency awarded a 10-year, US$4.7 billion contract to Russia’s largest state-owned internet service provider (ISP), Rostelecom, under which the company has committed to provide all settlements with a population of 250 to 500 people with points of internet access at speeds of at least 10 Mbps, entailing the installation of 200,000 km of fiber-optic cables. Internet access points will be established in more than 13,600 towns, reaching a total of some 4 million additional people.\(^11\)

**Restrictions on Connectivity**

During the coverage period, there were no government-imposed internet outages or disruptions to communication platforms. However, in two separate incidents in August 2015, the telecommunications authority banned articles on Wikipedia and Reddit (both related to recreational drug use),

---

\(^10\) Russian Association of Internet Communication and Higher School of Economics, *Economics of Runet*.
Russia

leading ISPs to temporarily block each platform in its entirety, since both employ HTTPS on their websites, which prevents ISPs from blocking individual pages.\textsuperscript{12}

In the summer of 2014, the Ministry of Communications announced the completion of a joint exercise with the Defense Ministry, the Interior Ministry, and the Federal Security Service (FSB), in which the authorities examined ways to disconnect Russia from the global internet. They tested the scenario of switching off the servers of the domains .RU and .РФ, which are located in Moscow, Novosibirsk, New York, Amsterdam, and Hong Kong. The exercise also simulated the deployment of an alternative system of domain-name servers hosted by Rostelecom. Officials claimed that the tests were only intended to prepare for cases in which the Russian internet is disconnected from the outside, on the initiative, for example, of the United States,\textsuperscript{13} but journalists, referring to sources in the ICT industry, said that a test for switching off the internet in Russia from the inside was also considered.\textsuperscript{14} At the same time, President Vladimir Putin made public statements declaring that Russia had no intention of limiting access to the internet. Given that Russia has over 300 companies that have purchased connectivity with outside providers, each of which would have to be shut off in order to completely disconnect the country from the global internet, it would be much more difficult for the Russian government to implement a so-called “kill switch” than it has been for other governments whose countries only had a few connections to the international infrastructure.\textsuperscript{15}

ICT Market

The communications market in Russia is still relatively concentrated among a few companies. The five largest operators control 67 percent of the market for broadband internet access. The state-owned Rostelecom controls 36 percent of the market, followed by TransTelecom, ER-Telecom, MTS, and Vimpel Communications (Beeline).\textsuperscript{16} The market for mobile phone access has become more concentrated over the past year: As of the fourth quarter of 2014, four major companies—Mobile TeleSystems, Megafon, Vimpel Communications, and Tele2—controlled 99 percent of the market, compared with 92 percent in 2013.\textsuperscript{17}

Regulatory Bodies

The ICT and media sector is regulated by the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), under the control of the Ministry of Communications and Mass Media. The head of Roskomnadzor, Aleksandr Zharov, was appointed by executive decree on May 3, 2012. Roskomnadzor is responsible for carrying out orders issued by the Prosecutor General’s Office to block content that is extremist or contains calls for participation in unsanctioned public actions, according to a new law that went into effect on February 1, 2014. As a result, Roskomnadzor has become a primary player in the field of controlling and filtering information on the internet.

\textsuperscript{13} Andrew Griffin, “Reddit banned in Russia because of one thread,” Independent, August 13, 2015, http://ind.pn/1PvYKzY
\textsuperscript{14} Nataliya Raibman, “Peskov: ‘Mad voices’ can demand to switch Russia off the internet” [in Russian], Vedomosti, October 1, 2014, http://bit.ly/1KhRXa
\textsuperscript{15} “Putin and Security Council will discuss Russia’s shutdown of the internet from outside” [in Russian], Forbes Russia, October 1, 2014, http://bit.ly/1LAgpSr
Limits on Content

The benefits of increases in access and the expansion of internet infrastructure have been offset by increasing censorship. The government continues to block websites based on an expanding list of restricted content. The leading independent online news outlets that were originally blocked in the spring of 2014 for their critical coverage of the Kremlin are still restricted, while others, facing economic pressure, have changed their editorial positions to become less critical of the government. In addition, the authorities are increasingly pressing large foreign companies like Google, Twitter, and Facebook to comply with content-removal demands. Meanwhile, the government actively manipulates public opinion through state-controlled media and paid commentators.

Blocking and Filtering

Since June 2014, the government has continued to block content related to antigovernment protests, the conflict in Ukraine, or support of opposition figures. This campaign of censorship began in earnest in March 2014, when, in the run-up to the Crimean secession referendum, the prosecutor general issued an order to block access to three major opposition websites—Grani.ru, a news site known for its criticism of the Kremlin, particularly the crackdown on and subsequent prosecution of participants in the 2012 Bolotnaya Square protests; Ezhednevny Zhurnal (Ej.ru), a news and opinion site; and Kasparov.ru, the website of former chess champion and current opposition figure Gary Kasparov. The owners of the websites were not provided with an explanation as to what content had violated the law and prompted the blocking order. At the same time, the authorities blocked access to the personal blog of opposition leader Aleksey Navalny and the website of the radio station Ekho Moskvy (Echo of Moscow), though these two were unblocked within a few days.

In December 2014, ahead of the sentencing of Navalny and his brother Oleg in what was widely seen as a trumped-up fraud case, Roskomnadzor issued a request to Facebook to block an event page for a planned protest on Moscow’s Manezh Square on January 15, which thousands of users had already indicated they would attend. Facebook initially complied with the request, though it refrained from blocking subsequent event pages. On December 30, when the sentencing was moved up in a bid to preempt the protests, Roskomnadzor issued warnings to four media outlets that reported on the sentencing and carried links to a video of Navalny calling for demonstrations. The agency claimed the sites had posted content that was inciting extremism.

Similarly, the former technical director of the social-networking site VKontakte, Nikolay Durov, reported that on December 21 the company had received 53 requests from Roskomnadzor to “block all pages, groups, and events that mention the name ‘Navalny.’”

From 2012 to 2013 the Russian government enacted legal amendments that gave several agen-

---

Russia

cies—including Roskomnadzor, the Prosecutor General’s Office, the Federal Service for Surveillance on Consumer Rights and Human Wellbeing (Rospotrebnadzor), and the Federal Drug Control Service—the authority to make decisions about blocking various categories of information. Currently, these agencies have the authority to block, without a court order, the following types of content: information about suicide, drug propaganda, child pornography, information about juvenile victims of crimes, materials that violate copyright, content related to extremism, and calls for unsanctioned public actions or rallies. Any other information may be blocked by a court decision, provided that the court finds the content illegal.

According to the nonprofit project RosComSvoboda, which conducts ongoing monitoring of blocked content, the following were blocked by the end of May 2015:

- 773 sites for extremism and calls for protests (by orders from the Prosecutor General’s Office)
- 3,981 sites containing drug-related content (by orders from the Federal Drug Control Service)
- 82 sites containing suicide propaganda (by the decision of Rospotrebnadzor)
- 2,613 sites for the distribution of child pornography (by the decision of Roskomnadzor)
- 2,701 sites, based on other court decisions, for the publication of various banned information

In most cases the legal framework offers no clear criteria for evaluating the legality of content, and public authorities do not always offer a detailed explanation for blocking decisions. The lack of precise guidelines sometimes leads telecom operators, which are responsible for complying with blocking orders, to carry out the widest blocking possible so as to avoid fines and threats to their licenses. Telecom operators are obliged to regularly consult the “blacklist” of banned websites, updated by Roskomnadzor. Moreover, the law does not specify how ISPs should restrict access; for example, based on the internet protocol (IP) address, the domain name, or the URL of the targeted page. Often the authorities do not consider it necessary to clearly indicate the specific pages that are meant to be blocked on a given site. As a result, entire sites, against which the authorities do not have any formal complaints, are often blocked. According to RosComSvoboda statistics, there are currently 262,991 websites that have been accidentally blocked due to blocking orders carried out on the basis of IP addresses.

Content Removal

The existing process for blocking online content, which only gives website owners a few hours or a few days to comply with the request, often leads them to delete the banned information rather than risk having the entire site blocked.

In cases where websites are registered as mass media, Roskomnadzor has additional powers to issue warnings to the editorial board about “abuse of freedom of mass media.” Article 4 of the law “On Mass Media” implies that such abuse can include, for example, incitement to terrorism, extremism, propaganda of violence and cruelty, information about illegal drugs, and obscene language. If a media outlet receives two warnings within a year, Roskomnadzor has the right to apply for a court order
to shut down the media outlet. Usually, the warnings from Roskomnadzor contain instructions to remove or edit the offending material. For example, in August 2014, at least 14 media outlets received warnings for publishing reports on a protest movement calling for greater regional autonomy, or “federalization,” particularly in Siberia. For instance, the magazine *New Times* was forced to remove from its website a large overview of the federalization phenomenon by journalist Aleksandr Litoy.

On December 30, 2014, Roskomnadzor issued warnings against four media outlets—Polit.ru, *Business Online*, BFM.ru, and *Mediazona*—for publishing materials containing “calls to change the constitutional order.” The content was actually a video of Aleksey Navalny’s speech after the verdict in the fraud case. In January 2015, at least six media outlets received warnings for publishing materials on that month’s terrorist attack against the French satirical magazine *Charlie Hebdo*, with Roskomnadzor issuing a formal statement that any cartoons on religious themes would be treated as extremism. Most of the media outlets that received these warnings chose to remove the materials.

According to Twitter’s Transparency Report covering July to December 2014, the company received 91 requests to remove information from Russian authorities, of which 13 percent were satisfied—two accounts and nine tweets were withheld. After the publication of the report, the head of Roskomnadzor publicly expressed dissatisfaction with the fact that Twitter was not fully cooperating and had refused to disclose user data or delete information at the request of Russian authorities. In the second half of 2014, Facebook limited access to 55 pieces of content “under local laws prohibiting content that promotes drug use and self-harm, extremist activities, unsanctioned mass riots/marches, and for violating the integrity of the Russian Federation.”

### Media, Diversity, and Content Manipulation

The online media environment is becoming more restricted as the government attempts to counteract information that might undermine its authority. While Russians are still able to access a wide variety of outside sources, many independent online media outlets within Russia have been forced to shut down over the past two years due to increasing pressure from the government, and pro-government trolling continues to be a problem. Self-censorship is encouraged by the vague wording of restrictive legislation, the seemingly arbitrary manner in which these laws are enforced, and the near-total ineffectiveness of judicial remedies. Laws prohibiting “extremist content” and the government’s crackdown on several media outlets have resulted in a chilling effect on free speech, particularly with regard to such sensitive topics as governance failures by the authorities, corruption, war with Ukraine, the annexation of Crimea, violation of civil rights, religion, and the LGBTI (lesbian, gay, bisexual, transgender, and intersex) community.

Several online media outlets that were originally blocked in March 2014 remain restricted. A number of other media outlets have received warnings from Roskomnadzor for their coverage of protests, the attack on *Charlie Hebdo*, or the criminal cases of Aleksey Navalny, meaning they run the risk of receiving a second warning and losing their licenses. While individuals are still able to use circum-
vention tools to access blocked content, officials at various levels have repeatedly spoken about the need to block access to such tools, though legislation to that effect has not yet been adopted. Despite the continued availability of circumvention tools, all blocked resources have reported a significant reduction in traffic.

In the spring of 2015, hackers published leaks of correspondence from the deputy head of the Office of Internal Policy of the Presidential Administration, which indicated that the administration is actively involved in a number of media outlets’ editorial policies and uses Roskomnadzor and the Prosecutor General’s Office to exert pressure on those who resist such directives.28

Russian authorities continue to use the assistance of paid commentators to influence online content. A 2013 investigation conducted by journalists at Novaya Gazeta showed that some members from the pro-Kremlin youth movements Nashi and Molodaya Gvardiya organized paid campaigns on social-networking sites.29 In January 2014, the editors of the German newspaper Die Zeit reported a wavelike increase in the number of anti-Western user comments, believed to be propaganda, on the paper’s website at the time of the Euromaidan protests in Ukraine.30 Other media outlets, including Forbes and the Guardian, reported a similar flood of “insulting, combative” comments on any articles related to Russia or Ukraine. In March 2015, journalists at Novaya Gazeta and the St. Petersburg outlet Moy Rayon published an investigation into the activity of pro-Kremlin paid commentators, revealing more than 500 accounts on the LiveJournal blogging platform that specialized in the publication of progovernment views and harassment of opposition activists.

Several new laws enacted during the coverage period also had the potential to restrict the information available online. In October 2014 Putin signed amendments to the law “On Mass Media” that prohibit foreign citizens and organizations from owning more than 20 percent stakes in Russian media; the changes are scheduled to take effect in January 2016, though outlets have until 2017 to reduce their existing foreign ownership. In May 2015, a new law on “undesirable organizations” included bans on disseminating information from the blacklisted organizations.

Data-localization laws can also have an impact on companies’ ability to operate within a given jurisdiction, and in July 2014 the Russian government enacted a law requiring technology companies processing Russians’ data to host the information on local servers. As international companies decided how and whether to comply with the law ahead of the September 1, 2015, deadline, some chose to reduce their presence in the country. In September 2014 the Russian branch of Adobe applied for liquidation.31 In November, Microsoft announced that it was closing its engineering office in Zelenograd and moving part of its staff to Prague.32 One month later, Google announced that it would also be closing its engineering offices in Russia.33

Digital Activism

Despite the continued government pressure, the internet in Russia remains the most versatile and

Russia

effective tool for activism. In 2014, social-networking sites were used successfully to organize public events. Some experts believe that the large groups that mobilized to demonstrate support for the Navalny brothers drove the courts to move up their sentencing date from January 15 to December 30—to preempt planned protests—and influenced the eventual outcome, in which Aleksey Navalny was sentenced to probation instead of imprisonment. Information about the protests spread on Facebook, Twitter, Vkontakte, Odnoklassniki, Google+, and other platforms, and demonstrations were organized in Moscow, Yekaterinburg, Perm, Novosibirsk, Berlin, New York, and London.

In addition to organizing protests via social media, Russians have continued to use crowdfunding as a tool for activism and mobilization. The crowdfunding platforms Planeta.ru and Boomstarter.ru have collected approximately US$7 million over two years to fund various community projects.

Violations of User Rights

The Russian government continues to enact laws that restrict online activity and increase the penalties for violations. In June 2014, the government passed amendments to the criminal code that set penalties of up to five years in prison for posting extremist content online. The amendments also made it illegal to finance an organization deemed extremist, with punishments including fines and prison terms. In addition, the authorities continue to expand their capacity for surveillance of ICTs, including through an update in April 2015 to the SORM surveillance system that incorporates DPI technology, allowing intelligence agents to access and search the content of online communications.

Legal Environment

Although the constitution grants the right to free speech, this right is routinely violated, and there are no special laws protecting online modes of expression. Online journalists do not possess the same rights as traditional journalists unless they register their websites as mass media. Russia remains a member of the Council of Europe and a party to the European Convention on Human Rights and Fundamental Freedoms, Article 10 of which enshrines the right to freedom of expression. However, over the past few years Russia has adopted a set of laws and other acts that, coupled with repressive law enforcement and judicial systems, have eroded freedom of expression in practice. Courts tend to side with the executive authorities, refusing to apply provisions of the constitution and international treaties that protect the basic rights of journalists and internet users.

Over the past year, the government passed amendments to significantly increase the penalties for online incitement to separatism or calls for extremism, with prison terms up to five years, and incitement to hatred, with prison terms up to six years. In addition to the criminal penalties, the mere opening of a criminal case could serve as a basis for the inclusion of the accused on a list of extremists maintained by the Federal Financial Monitoring Service. Individuals on this list, even if they have not been convicted, are restricted from certain professions, and their bank accounts can be frozen.

The law establishes criminal penalties for defamation (Article 128.1 of the criminal code), defamation against a judge or prosecutor (Article 298.1), insulting the authorities (Article 319), calls for terrorism or justification of terrorism (Article 205.1), insulting religious feelings (Article 148), calls for extremism (Article 280), calls for separatism (Article 280.1), incitement of hatred (Article 282), spreading false information on the activities of the Soviet Union in World War II, or insulting “symbols of Russian military glory” (Article 354.1). In addition, administrative prosecutions can be brought against
individuals for displaying Nazi symbols or symbols of organizations deemed extremist (Article 20.3 of the administrative code), the dissemination of extremist materials (Article 20.29), or insult (Article 5.61).

Prosecutions and Detentions for Online Activities

According to the SOVA analytical center, dozens of activists, journalists, and online editors continue to be subjected to administrative and criminal prosecution for content they post online. The majority of cases result in penalties such as fines and suspended sentences. However, the possibility of criminal prosecution even for reposting an item deemed to contain extremist content has had a significant chilling effect, with users apparently more inhibited in discussing political and social issues online.

There were several arrests and sentences over the past year for online activities falling under Article 280 (calls for extremism) and Article 282 (incitement of hatred):

- In December 2014, the chairman of the Tatar Public Center, Rafis Kashapov, was arrested in Kazan on charges of inciting hatred. The arrest was prompted by Kashapov’s posts on Vkontakte, which supported Ukraine and the Crimean Tatars while condemning the illegal annexation of Crimea and the actions of Russian authorities. In September 2015, Kashapov was sentenced to three years in prison.

- Krasnodar activist Darya Polyudova was arrested in August 2014 and spent six months in pretrial detention for using Vkontakte to call for a march demanding the federalization of Kuban, which was never held. According to Radio Free Europe/Radio Liberty, Polyudova was charged with promoting separatism and faces up to five years in prison.

- In May 2015, LGBTI activist and environmentalist Konstantin Golava was arrested on charges of incitement and extremism. The arrest stemmed from antigovernment posts on VKontakte that were deemed extremist. He was released pending trial.

- Sergey Reznik, a freelance blogger imprisoned since November 2013, was charged for a second time in July 2014 for allegedly insulting authorities online. The prosecution did not specify which blog posts on his LiveJournal account were being investigated. In January 2015, Reznik was sentenced to an additional three years in prison.

There were a number of other cases related to the dissemination of banned symbols or extremist materials online. More than a dozen users from various regions of Russia were prosecuted in 2014 under Article 20 of the administrative code for circulating a video, originally published in 2011, that

---

criticized the ruling United Russia party. The video was deemed extremist in 2013, and the prosecutor’s office indicted individuals who “liked” or reposted the video in 2014, with some cases resulting in fines.

Several individuals have also been questioned or fined for posting material that references Nazi symbols. In March 2015, a court in Ulan-Ude fined Mariya Burdakovskaya RUB 1,000 (US$20) for posting an image on VKontakte of a Nazi-style eagle over the phrase “grammar will make you free”—a reference to a joke about “grammar Nazis.” Also in March 2015, Readovka.ru correspondent Polina Petruzeva was fined RUB 1,000 (US$20) for circulating a photograph on VKontakte of the German occupation of Smolensk during World War II. The photo depicted the house where the journalist is now living with a Nazi flag and swastika.

**Surveillance, Privacy, and Anonymity**

Over the past year, the Russian authorities have actively tried to limit internet users’ ability to remain anonymous online, while simultaneously expanding the government’s capacity for surveillance. The July 2014 data localization law, which requires all foreign internet companies to host Russians’ data on servers within the country, could facilitate the Russian government’s access to user data. In May 2014, Putin had signed a law that considered any website with over 3,000 daily viewers, including blogs and social media accounts, to be “mass media,” requiring them to register with the government; among other effects, this decreased the space for users to communicate anonymously online. The measure also contained wording that would require any services hosting such outlets to maintain records of their data on servers located within Russia. As of May 2015, more than 700 popular bloggers were included on the list.

In July 2014, the Ministry of Communications issued an order regarding the new requirements for ISPs to update their equipment for the implementation of SORM, the system used by the security services to carry out surveillance. As of March 31, 2015, ISPs in Russia were required to upgrade to SORM-3, which uses DPI technology, enhancing the ability of the security services to monitor content on all telecommunications networks in Russia.

SORM, or “system for operational investigative measures,” has been gradually improved since it was first launched in the late 1990s. Indeed, there is evidence that the Russian government has significantly increased its overall surveillance capabilities over the past few years. Procurement documents revealed the extent to which the government had expanded its domestic surveillance infrastructure, including upgrades to telephone and Wi-Fi networks, ahead of the February 2014 Winter Olympic Games in Sochi. Such technology has been used for political purposes in the past, including the

---

targeting of opposition leaders. In a Supreme Court case in November 2012 involving Maksim Petlin, an opposition leader in the city of Yekaterinburg, the court upheld the government’s right to eavesdrop on Petlin’s phone conversations because he had taken part in “extremist activities,” namely antigovernment protests. Online surveillance represents somewhat less of a threat in the major cities of Moscow and St. Petersburg than in the regions, where almost every significant blog or forum is monitored by the local police and prosecutor’s office. Most of the harassment suffered by critical bloggers and other online activists in Russia occurs in the regions.

Under current legislation, in order to receive an operating license, ISPs are required to install equipment that allows security services to monitor internet traffic. ISPs that do not comply with SORM system requirements are promptly fined, and may have their licenses revoked if problems persist. Russian authorities are technically required to obtain a court order before accessing an individual’s electronic communications data; however, the authorities are not required to show the warrant to ISPs or telecom providers, and FSB officers have direct access to operators’ servers through local control centers. Experts note that there is no information about any government efforts to punish security officers who abuse tracking methods.47 ISPs and mobile providers are required to grant network access to law enforcement agencies conducting search operations, and to turn over other information requested by the prosecutor’s office, the Interior Ministry, the FSB, or the Investigative Committee.

There are currently no explicit restrictions on the use of circumvention tools or anonymizers, though such tools may be banned in the near future. Russian officials have periodically proposed the idea of prohibiting the use of anonymizers and proxy servers, and in August 2013 it was reported that the FSB was developing a package of laws to block access to Tor and foreign proxy servers for Russian users.48 In April 2015, a court issued a decision to block the website of RosKomSvoboda, which provided instructions on how to use circumvention tools. The ruling stated that the website “is an anonymizer,” which is incorrect, and anonymizing tools are not currently banned in any case.49

Presently, identification is needed to sign a contract for internet access or mobile service. In addition, owners of public Wi-Fi facilities are required to use content filters to protect children from potentially “harmful” information. This requirement may force owners to implement age checks for users. As of April 2015, according to the Department of Information Technology in Moscow, identification was required for use of all public Wi-Fi networks in the city.50

**Intimidation and Violence**

Impunity flourishes in Russia, and perpetrators of attacks on online activists and bloggers continue to avoid prosecution.51 The failure of the authorities to protect activists and uphold international human rights standards have set dangerous precedents that foster a climate of intimidation.52 Investigations into past attacks, such as the 2011 murder of Chernovik founder Gadzhimurad Kamalov and

50 Rublblacklist, “There will be no anonymous access to public Wi-Fi in Moscow” [in Russian], March 2, 2015, [http://bit.ly/1JnG-1Dk](http://bit.ly/1JnG-1Dk).
the 2013 murder of Caucasian Knot journalist Akhmednabi Akhmednabiyev, have been suspended or remain ineffective.\textsuperscript{53}

In August 2014, Timur Kuashev, a blogger for Kavkazkaya Politika (Caucasian Politics), Caucasian Knot, and Dosh, was found dead on the outskirts of Nalchik.\textsuperscript{54} Kuashev’s writings criticized the actions of local government and law enforcement officials.\textsuperscript{55} In January 2015, Sergey Vilkov, a journalist for the independent news website Obschestvennoye Mneniye (Public Opinion), was assaulted in Saratov. The attack was apparently motivated by Vilkov’s investigative reports on government corruption and organized crime in the region.\textsuperscript{56} Vyacheslav Starodubets, a Dagestan-based blogger and founder of My Derbent, a website reporting on local corruption, was kidnapped, badly beaten, and hospitalized in April 2015.\textsuperscript{57}

The threat of harassment, violence, or criminal prosecution has forced some activists and bloggers to flee the country. In November 2014, Altai activist Andrey Teslenko, accused of provoking hatred online, was granted asylum in Ukraine.\textsuperscript{58} Teslenko had reposted an article on VKontakte that criticized Russia’s call for Ukraine to crack down on protesters during the Euromaidan protests. In an earlier case, Maksim Yefimov, a human rights defender and journalist, was granted asylum in Estonia in 2012. He is currently being investigated under Article 282.1 of the criminal code over an editorial he published that condemned corruption within Russia’s Orthodox Church.\textsuperscript{59}

In August 2014, eight journalists were violently attacked or otherwise obstructed in Pskov, apparently in connection with their investigations into the burials of paratroopers who were allegedly killed in eastern Ukraine, despite the Russian government’s denial that any troops were deployed there. In one incident, four journalists—Vladimir Romensky of TV Dozhd, Ilya Vasyunin of Russkaya Planeta, Nina Petlyanova of Novaya Gazeta, and Irina Tumakova of the website Fontanka.ru—were attacked by unidentified assailants.\textsuperscript{60} The group was visiting the site of the secret burials when the attackers attempted to break their car’s windows and slit its tires.\textsuperscript{61} The assault was documented on video, and an investigation was launched following pressure from the Russian Council for Civil Society and Human Rights.

### Technical Attacks

Cyberattacks against independent media, blogs, and news portals continue to inhibit Russian internet users’ ability to access such sites. In September 2014, Google notified several of its Russian users...
that anonymous hackers from an unnamed state were trying to access their accounts.\textsuperscript{62} The news portal Kasparov.ru, which had already been blocked for internet users within Russia in March 2014, reported two massive distributed denial-of-service (DDoS) attacks against its website in May 2015.\textsuperscript{63}

In previous years, websites that suffered DDoS attacks included the internet project Demokrator.ru, Saint Petersburg news portals Zaks.ru and Lenizdat.ru, the website of the SOVA Center for Information and Analysis, the website of the daily newspaper Moskovsky Komsomolets, the Murmansk-based portal Bloger51.ru, and the websites of Novaya Gazeta and TV Dozhd.

\textsuperscript{62} Irina Yuzbekova and Roman Dorokhov, “Google notified its Russian users about an attack” [in Russian], RBC, September 9, 2014, \url{http://bit.ly/11AZa1X}

\textsuperscript{63} “Kasparov.ru under second DDoS attack” [in Russian], Grani, May 28, 2015, \url{http://bit.ly/1OPYQku}
Rwanda

Key Developments: June 2014 – May 2015

- As a result of the government’s commitment to ICT development, the Alliance for Affordable Internet listed Rwanda as the top-ranked developing country in its 2014 Affordability Index (see Availability and Ease of Access).

- Three BBC websites were blocked in October 2014 in response to the BBC’s broadcast of the controversial documentary, “Rwanda, The Untold Story” (see Blocking and Filtering).

- Popular singer Kizito Mihigo was sentenced to 10 years in prison in February 2015 after he was found guilty of conspiring to overthrow the government in a trial that used his private WhatsApp and Skype messages to alleged opposition critics in exile against him as evidence (see Surveillance, Privacy, and Anonymity).
Rwanda

Introduction

In the past year, the government of Rwanda under President Paul Kagame intensified its ambitious economic development strategy that aims to create a vibrant industry for information and communication technologies (ICTs) and position Rwanda as a regional ICT hub. Although internet penetration remained low—hampered primarily by poverty and a lack of appropriate infrastructure, especially in rural areas—access continually expanded due to public and private investments in broadband technology across the country, while mobile internet access increased at an impressive rate.

Despite progress in ICT access, the country's tenuous political environment and sensitive ethnic relations since the 1994 genocide has led the government to exert some controls over online content and expression. Throughout 2014 and 2015, a number of independent online news outlets and critical blogs remained unavailable, joined by three BBC websites in October 2014 following the government's outcry against the television broadcast of the documentary, "Rwanda, The Untold Story." Though the documentary had not been aired in Rwanda, the government immediately suspended the BBC radio and web services, accusing the media outlet of "genocide denial," a crime under the country's harsh media laws.

Given the country's restrictive political environment, there is a strong sense that government surveillance over online communications has been increasing with little oversight. In April 2014, the government's abuse of its surveillance powers was revealed in the trial against popular singer Kizito Mihigo, who's private WhatsApp and Skype messages with alleged opposition critics in exile were used against him as evidence to convict him of conspiracy to overthrow the government. The incident led to revelations among ordinary Rwandans that their private communications are not safe. He was sentenced in February 2015 to 10 years in prison.

Obstacles to Access

As a result of the government's commitment to ICT development, the Alliance for Affordable Internet listed Rwanda as the top-ranked developing country in its 2014 Affordability Index. The regulator's lack of independence was revealed in its decision to ban BBC broadcast radio and websites in October 2014.

Availability and Ease of Access

Although Rwanda has made major strides in expanding access to ICTs across the country, poverty continues to be the primary impediment to ICT uptake, especially the internet. Over 90 percent of the population lives in rural areas, with the majority practicing subsistence agriculture and approximately 45 percent still living below the poverty line. Consequently, internet penetration in Rwanda is still low at 11 percent in 2014, up from 9 percent in 2013, according to the International Telecommunication Union (ITU). By contrast, official government statistics cite an internet penetration rate of over 28 percent as of March 2015, which includes internet subscriptions on mobile devices. In

---

Rwanda

fact, mobile internet comprises over 99 percent of all internet subscriptions, while fixed-line internet subscriptions make up less than 1 percent in Rwanda.

Mobile phone penetration is significantly higher than that for internet access at 64 percent in 2014, according to the ITU, while government figures noted a penetration rate of 71 percent as of March 2015. Rural populations have a relatively high mobile phone usage rate compared to rural internet access rates, as access has been made easier by a well-developed mobile phone network that covers nearly 100 percent of the population. Innovative initiatives targeting rural populations have encouraged increased mobile phone and internet usage, such as the e-Soko (“e-market”) program created by the Rwanda Development Board, which provides farmers with real-time information about market prices for their agricultural produce on their mobile devices.

Internet access is still concentrated primarily in Kigali, the capital city, and remains beyond the economic reach of most citizens, particularly those in rural areas who are limited by low disposable incomes and do not have high levels of ICT awareness. In addition, only 11 percent of Rwandans are ICT literate and over 70 percent of the population speaks only Kinyarwanda, making internet content in English inaccessible to the majority of Rwandans. Only 17 percent of Rwandan households have regular access to electricity.

In the face of such challenges, the Rwandan government has made ICT development a high priority. Fixed-broadband internet services are expanding across the country, resulting in increasing speeds. According to May 2015 data, from Akamai’s State of the Internet report, Rwanda’s average internet connection speed was 5.8 Mbps (compared to a global average of 3.9 Mbps), up from 1.4 Mbps the previous year.

As a result of Rwanda’s commitment to ICT development, the cost of access has continually decreased, leading the Alliance for Affordable Internet to list Rwanda as the top-ranked developing country in its 2014 Affordability Index. As of early 2015, a 128/64 Kbps package of wireless internet cost about RWF 64,900 (US$95). While still prohibitively expensive for average citizens, the cost is a significant reduction from before the country’s fiber-optic cable installation in 2011, when 1 megabyte of internet access reportedly cost US$2,000. Meanwhile, the cost of using the internet in a cybercafe is approximately US$0.14 (RWF 100) for 1 hour. The cost of internet access via mobile

---

phones has also declined, helping fuel the exponential growth of mobile internet users. As of March 2015, mobile internet tariffs range from RWF 50 to 55 per Mb (US$0.03 to $0.08 per Mb).16

Restrictions on Connectivity

There were no restrictions on connectivity reported in Rwanda during the coverage period, though Article 52 of the 2001 Law Governing Telecommunications gives the government sweeping powers over telecommunications networks in the name of preserving "national integrity." These powers include the ability to “suspend a telecommunications service for an indeterminate period, either generally or for certain communications.”17 Furthermore, the government possesses some control over the country's internet infrastructure, which may provide the authorities with the ability to restrict access at will. According to the ITU, the level of competition for Rwanda's international gateway is characterized as "partial."18

The local internet exchange point (IXP), the Rwanda Internet Exchange (RINEX),19 is managed by the Rwanda Information & Communications Technology Association, a non-profit comprised of ICT institutions and professionals.20 As of mid-2015, five of Rwanda's nine ISPs exchange internet traffic through RINEX, and ISPs can also opt to connect via RINEX to the international internet.21

ICT Market

Rwanda's ICT market is vibrant and competitive, with no reported interference from the government. Following the country's market liberalization policies implemented in 2001,22 the number of companies providing telephone and internet services increased from one—the state-run Rwandatel23—to nine ISPs and three mobile phone companies in 2015,24 all of which are privately owned. The three main mobile phone operators are MTN, TIGO, and Airtel, whose respective market shares are 49 percent, 35 percent, and 16 percent.25

In December 2014, the government of Rwanda launched a partnership with the Korean Embassy to initiate a 4G LTE network, which is expected to offer the fastest wireless communication on high-speed data for mobile phones and internet-enabled devices.26

---

16 RURA, "Statistics and Tariff Information in Telecom Sector as of March 2015."
23 In 2012, Rwandatel was liquidated; its assets were purchased by Tigo and Airtel, and the company was taken over by the Government of Rwanda. See, Shyaka Kanuma, “Bye Bye Rwandatel,” Rwanda Focus, February 20, 2012, http://bit.ly/2OyDakR.
24 These include fixed-line providers (Liquid Telecom and MTN Rwanda), mobile phone providers (MTN Rwandacell, TIGO and AIRTEL), and internet service providers (MTN Rwanda, Liquid Telecom, TIGO Rwanda, New Artel, ISPA, 4G Networks, BSC, Airtel Rwanda, and AXOIM). See: RURA, "Statistics and Tariff Information in Telecom Sector as of March 2014."
Rwanda

Regulatory Bodies

The Rwanda Utilities Regulatory Agency (RURA) oversees the regulatory frameworks and implementation of the country’s policies and strategies in the telecommunications sector. Officially, RURA is a national body with autonomy in its administrative and financial management. Nevertheless, the government audits RURA’s budget while the president nominates its seven board members, supervisory board, and director general who all work under full control of the government.

In 2015, RURA demonstrated its allegiance to the government in its decision to indefinitely ban the British Broadcasting Corporation’s (BBC) radio services and block BBC websites following the October 2014 broadcast of a controversial documentary titled, “Rwanda, The Untold Story” (see “Blocking and Filtering”). The incident also saw RURA’s silencing of the media self-regulatory body, the Rwanda Media Commission (RMC), which the government proposed to take over as a state-run entity after the then-RMC head, Fred Muvunyi, made vocal objections to the BBC ban. Muvunyi subsequently fled the country in May 2015 after months of threats and intimidation.

Limits on Content

Three BBC websites joined the list of websites blocked in Rwanda, which includes numerous independent news outlets and opposition blogs that have been blocked for years.

Blocking and Filtering

While the Rwandan government has demonstrated a commitment to expanding access to ICTs across the country, it has also simultaneously endeavored to restrict the types of content that users can access, particularly content of oppositional nature. A study conducted in early 2015 found that the websites of numerous independent news outlets and opposition blogs that have been blocked for years—such as the websites of Inyenyeri News, Veritas Info, The Rwandan, and Leprophete—remained inaccessible in Rwanda, among others. There is no transparency behind the government’s blocking decisions and no avenues for appeal.

In late 2014, the BBC was added to the list of websites blocked in Rwanda following the government’s outcry against the television broadcast of the documentary, “Rwanda, The Untold Story,” in October 2014, which argued that the number of Hutus who died during the genocide was much higher than officially recognized. Though the documentary had not been aired in Rwanda, the government immediately suspended the BBC’s popular radio services, accusing the media outlet of “genocide denial,” a crime under the country’s harsh media laws. The regulator RURA indefinitely

30 Sue Valentine, “Hopes of independent press in Rwanda fade as head of media body flees,” Committee to Protect Journalists (blog), July 8, 2015, https://cpj.org/x/64d5.
31 Study conducted by Freedom House consultant, March 2015.
32 Other opposition blog websites that were unavailable as of May 2015 were: http://www.iwacu.com; http://www.musabyimana.be; http://rwandarwabanyarwanda.over-blog.com; http://www.banyarwandapoliticalparty.org.
Rwanda

banned BBC broadcasts in May 2015.\(^{34}\) BBC websites, including BBC Swahili, BBC Africa, and BBC Afrique were also blocked as part of the government’s crackdown on the BBC.\(^{35}\)

Despite the increasing blocks on certain websites, social-networking sites such as YouTube, Facebook, Twitter, and international blog-hosting services are freely available. Given the more restricted space for press freedom in the traditional media sphere, Rwandan media outlets are increasingly going online to bypass government control or suspension as well as heavy production costs.\(^{36}\)

Content Removal

The extent to which the government forces websites to delete certain content is unknown, though anecdotal incidents over the past few years suggest that some degree of forced content removal by the state exists, and that such ad hoc requirements lack transparency.\(^{37}\)

According to a 2010 law relating to electronic messages, signatures, and transactions, intermediaries and service providers are not held liable for the content transmitted through their networks.\(^{38}\) Nonetheless, service providers are required to taken down content when handed a takedown notice, and there are no avenues for appeal.

Media, Diversity, and Content Manipulation

The Rwandan government’s heavy-handed repression of the media has severely limited the diversity of the information landscape in the country, both online and offline. Critical and independent online news generally stem from opposition supporters living outside Rwanda—mainly in Europe, the United States, and South Africa—and are blocked in Rwanda. Few Rwandans in the country are aware of the critical content that is unavailable to them.

Online news outlets based in the country frequently contend with editorial interference by security officials and other government authorities who impose “red lines” on what can and cannot be published.\(^{39}\) The recent spate of extrajudicial killings across the country was one of the main “red lines” drawn in the past year. Independent outlets also face economic challenges in comparison to their state-run counterparts that receive income from government advertisements and direct subsidies.

As a result of the high degree of repression, online journalists based in the country are increasingly joining their print and broadcast colleagues in exercising self-censorship, particularly on topics that can be construed as disruptive to national unity and reconciliation.\(^{40}\) In addition, issues related to the military and national security are highly sensitive and subject to restrictions regarding the right to

---

\(^{34}\) RURA, “Decision N˚…/RURA/2015 of 29 May, 2015 on the Inquiry Into the Documentary Aired By BBC: ‘Rwanda’s Untold Story’.”


\(^{37}\) Two online news websites, Umusingi and Umurabyo, had reported experiencing such requests to delete content related to local political affairs and ethnic relations in previous years.


\(^{39}\) According to online journalists who were contacted for the study but who requested anonymity.

Rwanda

access information. According to some journalists, self-censorship is viewed as a legitimate practice given the country’s sensitive social and political environment, though others believe that the ruling Rwandan Patriotic Front (RPF) uses “repression, social pressure, and self-censorship” to determine what is politically correct and to shape public opinion.

Despite the lack of diversity in online content, Rwandans are active on Facebook and Twitter, which have become popular platforms for online interaction as a result of the increasing use of internet-enabled phones. President Kagame is an active supporter of social networking websites, occasionally using the platforms to engage in discussions with users and openly respond to issues concerning the current state of governance in the country. Various government officials are also very active in social media, especially on Twitter.

The popularity of social media platforms has grown in tandem with the activity of progovernment trolls that work to harass independent journalists and manipulate online content. In 2014, revelations of such surfaced when an international journalist for Radio France Internationale, Sonia Rolley, was repeatedly harassed on Twitter by a user known as @RichardGoldston. Rolley had been reporting on the mysterious January 1, 2014 assassination of Patrick Karegeya, a former top intelligence official in Kagame’s inner circle who had been living in exile in Johannesburg. It was later revealed on the official Twitter account of Paul Kagame’s office (@UrugwiroVillage) that “@RichardGoldson was an unauthorized account run by an employee in the Presidency.” Another foreign correspondent, Steve Terrill, who used Twitter to publicly call on @RichardGoldston to end the harassment, was subsequently barred from entering Kigali in March 2014 to cover the 20th anniversary of the Rwandan genocide.

Digital Activism

Digital activism over political and social issues is not common in Rwanda. Nevertheless, the use of mobile phones to engage with popular radio programs has become an important medium for citizens to anonymously voice discontent with the authorities and expose abuses of power. For example, the live-radio programs, “Good Morning Rwanda” and “Good Evening Rwanda,” are significant venues for citizens to criticize government malpractices via SMS messages and voice calls, which are broadcast on the radio. However, given SIM card registration requirements, users have become less intent on engaging in very critical or sensitive discussions out of fear of being identified.

Violations of User Rights

Popular singer Kizito Mihigo was sentenced to 10 years in prison in February 2015 after he was found
Rwanda

guilty of conspiring to overthrow the government in a trial that used his private WhatsApp and Skype messages to alleged opposition critics in exile against him as evidence.

Legal Environment

The Rwandan constitution, adopted in May 2003, provides for freedom of the press and freedom of information, but in practice, the government maintains tight control over the media. The Rwandan judiciary is not fully independent, and many journalists view the threat of imprisonment as a key constraint on their work.

In a positive step, the state adopted progressive amendments to the 2009 Media Law in March 2013, granting journalists the “right to seek, receive, give and broadcast information and ideas through media,” and explicitly provided for freedom of online communications in Section 3, Article 19. The new law was also commended for providing for media self-regulation under the new Rwanda Media Commission and was viewed favorably by local journalists, who hoped that its passage would spell the end of government interference in the work of journalists and boost media freedom in Rwanda.

However, the new law also increased the government ability to control the internet by giving the minister of ICTs unlimited powers to establish the conditions for both local and foreign media companies to operate in Rwanda.

While there are no laws that specifically restrict internet content or criminalize online expression, Rwanda’s generally restrictive legal provisions governing the traditional media can be applied to the internet. Penalties for criminal defamation may also be applicable to the internet, with defamation of the president or other public officials carrying a penalty of up to five years in prison. October 2013 amendments to the law against “genocide ideology” similarly threatens freedom of expression both online and off, prescribing heavy prison sentences of up to 9 years and fines for any offender “... who disseminates genocide ideology in public through documents, speeches, pictures, media or any other means.”

The law also excludes a clear distinction between a private conversation and public speech.

Prosecutions and Detentions for Online Activities

Arrests and prosecutions for online activities are not common in Rwanda, in large part due to the lack of critical commentary originating in the country and the high degree of self-censorship practiced by online journalists and ordinary users alike. The last arrest occurred in April 2014, when the editor of the independent news website Umusingi, Stanley Gatera, was arrested on trumped-up charges of attempted extortion. He was previously convicted and sentenced to one year in prison in November 2012 on charges of divisionism and sectarianism for an article he published in Umusingi.

Rwanda

He was released in July 2013 only to be targeted again for arrest less than a year later, which the journalist believed was linked to an interview he conducted on Al Jazeera’s *People and Power* program—posted online and broadcast on television—in March 2014 in which he spoke about the difficulties journalists face while working in Rwanda. Gatera was held for six hours in April and received death threats after his release.

**Surveillance, Privacy, and Anonymity**

The sophistication of the Rwandan authorities’ surveillance capabilities is unknown, but there is growing suspicion that surveillance is pervasive, particularly after increasing revelations of attacks and assassinations of exiled Rwandan dissidents by the Kagame regime, despite their efforts to protect their identities, over the past couple of years. In July 2015, email leaks from the Italian surveillance firm Hacking Team revealed that the Rwandan government attempted to purchase the company’s sophisticated spyware known as Remote Control System (RCS) in 2012. While the leaked emails did not confirm the sale, they point to the government’s intent to acquire such technologies that can monitor and intercept user communications.

The government’s surveillance powers were expanded in October 2013 under amendments to the 2008 Law Relating to the Interception of Communications, which authorizes high-ranking security officials to tap into the communications, both online and offline, of individuals considered potential threats to “public security.” Under the amendments, communications service providers are required to ensure that their systems have the technical capability to intercept communications upon demand, though security officials also have the power to “intercept communications using equipment that is not facilitated by communication service providers,” which de facto allows the authorities to hack into a telecommunications network without a provider’s knowledge or assistance.

The law requires government officials to apply for an interception warrant, warrants are issued by the national prosecutor, who is appointed by the justice minister. The national prosecutor can also issue warrants verbally in urgent security matters, to be followed by a written warrant within 24 hours.

In April 2014, a glimpse into the government’s abuse of its surveillance powers was revealed in the trial against popular singer Kizito Mihigo, who’s private WhatsApp and Skype messages with alleged opposition critics in exile were used against him as evidence to convict him of conspiracy to overthrow the government. The incident led to revelations among ordinary Rwandans that their private communications are not safe. Mihigo was sentenced in February 2015 to 10 years in prison.

---

55 Committee to Protect Journalists, “Two journalists released from prison in Rwanda,” August 9, 2013, [https://cpj.org/x/5687](https://cpj.org/x/5687).
60 “Law Relating to the Interception of Communications” Official Gazette nº 41 of 14/10/2013.
64 “Rwanda singer Kizito Mihigo planned to kill Paul Kagame,” BBC, February 27, 2015, [http://bbc.in/1LT971S](http://bbc.in/1LT971S).
Rwanda

The ability to communicate anonymously is compromised by mandatory SIM card registration requirements initiated in early 2013. Under the regulation establishing SIM card registration, the ICT regulator RURA is given unfettered access to SIM card databases managed by operators, while other “authorized” individuals or institutions may also be granted access.

The various legal provisions that enable surveillance and limit anonymity are particularly troubling in the absence of a comprehensive data protection law that can safeguard citizens’ private data. A data protection law was drafted in July 2013, though the draft law provides exceptions to user data protections in the vaguely defined interest of national sovereignty, national security, and public policy, which may pose a threat to individuals critical of the regime. There has been no movement on the passage of the draft law as of mid-2015.

Intimidation and Violence

Critical journalists within the country frequently face violence and harassment when attempting to cover news stories, leading many to flee the country and report in exile. According to the Committee to Protect Journalists, Rwanda ranks among the top 10 countries from which journalists seek exile. Online journalists and ordinary users, however, have not yet experienced the same level of intimidation as traditional media journalists to date, likely as a result of high levels of self-censorship.

No Rwandan journalists have been killed since 2011, when the editor of the independent news website Inyenyeri News, Charles Ingabire, was gunned down in Kampala. Worryingly, the brother of Umuvugizi news website editor John Bosco Gasasira (in exile in Sweden), Andrew Muhanguzi was reported missing in February 2014. His family claims that Muhanguzi was kidnapped by men in Ugandan police uniforms outside their home on February 16, but the Ugandan police stated they have no record of his arrest. Muhanguzi and his family had left Rwanda in 2012 to escape alleged harassment by the Rwandan authorities for their relationship to John Bosco Gasasira and the critical Umuvugizi online newspaper.

Technical Attacks

Technical attacks against online news outlets and websites of human rights organizations are not common but arise occasionally. The last reported attack occurred in April 2014, when the investigative news website, Irene, experienced a seemingly targeted cyberattack, though the source of the attack was unknown.

66 See Regulations on SIM Card Registration, art. 13 and 15, http://bit.ly/1VWMi8w
68 Human Rights Watch, “Rwanda: Repression Across Borders.”
73 Risdel Kasasira and Solomon Arinaitwe, “Exiled Rwandan journalist brother feared kidnapped in Kampala.”
74 Reporters Without Borders, “Wave of intimidation of Kigali media.”
Saudi Arabia

Key Developments: June 2014 – May 2015

- The Saudi television channel Rotana ordered Google to take down a video of the satirical YouTube show "Fitnah" on copyright grounds, after the show had used footage from Rotana to criticize its owner, Prince Waleed bin Talal. The video was later restored by YouTube (see \textit{Content Removals}).

- Human rights activists Waleed Abu al-Khair and Fowzan al-Harbi have had their prison sentences extended to 15 and 10 years, respectively, upon appeals by the public prosecutor (see \textit{Prosecutions and Detentions for Online Activities}).

- Raif Badawi, who co-founded the website Saudi Arabia Liberals, had his 10-year sentence suspended and later upheld by the Supreme Court and received the first set of 50 lashes in January. He was sentenced to a total 1,000 lashes, to be carried out in public (see \textit{Prosecutions and Detentions for Online Activities}).

- During a funeral for the victims of an attack by Islamic State (IS) militants on a Shiite mosque, political activist Waleed Sulais was beaten by two men who accused him of insulting them on social networks (see \textit{Intimidation and Violence}).
Saudi Arabia

Introduction

The repression of Saudi Arabia’s online sphere showed no signs of letting up with the accession of King Salman bin Abdulaziz al-Saud to the throne in January 2015. The Saudi government continues to promote the internet use as a tool for economic development and e-government services, where it is ahead of many countries in the region. Mobile broadband penetration increased, Saudis remain the some of the most active users of social media in the world, and new tools for encrypting web traffic and circumventing state censorship have provided Saudi internet users with opportunities to access a greater array of information and to express themselves on certain topics. Following Salman’s appointment, the Twitter account @KingSalman received some 2 million new followers in six months. While the internet remains the least repressive space for expression in the country, it is by no means free, as evidenced by the numerous violations of users’ rights that took place over the past year.

Given the significance and relevance that social media has taken on in the country, authorities have not turned a blind eye to critical voices or liberal commentary. While the state focuses on combating violent extremism and disrupting terrorist networks, it has clamped down on nonviolent liberal activists and human rights defenders with the same zeal, branding them a threat to the national order and prosecuting them in special terrorism tribunals. Waleed Abu al-Khair, Fowzan al-Harbi, Abdullah al-Hamid, Mohammed al-Qahtani, and Raif Badawi are all serving prison sentences of 10 years or longer, with charges relating in part to their online activities. Many other prisoners of conscience have been held for years without trial, according to a recent law that removed restrictions on arbitrary detention.

The repression has been institutionalized under antiterrorism and cybercrimes that have instilled fear into activists and ordinary social media users alike, creating an environment of pervasive self-censorship. Surveillance, too, has a chilling effect; social media is heavily monitored and law enforcement agencies have sought to break or bypass encryption in order to spy on users. While the internet has fundamentally changed the way that young Saudis interact with each other, the authoritarian tendencies of the country’s political and religious establishments remain fully present in the minds of internet users, whose democratic aspirations remain blocked.

Obstacles to Access

Overall, infrastructure is not considered a major barrier to access except in remote and sparsely populated areas. Internet penetration is highest in major cities such as Riyadh and Jeddah, as well as in the oil-rich Eastern Province. Young Saudis make up the majority of the user population throughout the country. Arabic content is widely available, as are Arabic versions of applications such as chat rooms, discussion forums, and social media sites.

3 As of April 2015: King Salman, Twitter profile, https://twitter.com/kingsalman.
Availability and Ease of Access

Saudis have enjoyed a rapid growth of internet and communications technologies (ICTs) in recent years. Access increased to 63.7 percent of the population by the end of 2014, up from 38 percent in 2009. Saudi Arabia is home to around 19.6 million internet users. Fixed broadband subscriptions stood at 43.2 percent of all households, with a majority using ADSL connections. Monthly expenditure on 4G broadband ranges from between SAR 55 (US$11) for a 2GB allowance to SAR 95 (US$25) for a 20GB allowance. Household internet plus television packages with fiber-optic connections range from SAR 300 (US$80) for speeds of 25 Mbps to SAR 800 (US$213) for 200 Mbps.

Mobile broadband penetration has jumped from 47.6 percent to 94.5 percent from 2013 to 2014, with some 29 million mobile broadband subscriptions. Standard mobile phone subscriptions have risen to 53 million, resulting in a penetration rate of 171.4 percent. Finally, 87 percent of mobile subscriptions are prepaid. The number of mobile subscriptions has dropped from a height of 56 million in 2011 as the government deported thousands of illegal workers and deactivated prepaid mobile accounts whose owners are not in the country legally.

Restrictions on Connectivity

Saudi Arabia is connected to the internet through two country-level data services providers, the Integrated Telecom Company and Bayanat al-Oula for Network Services, up from a single gateway in years past. These servers, which contain long lists of blocked sites, are placed between the state-owned internet backbone and global servers. All user requests that arrive via Saudi internet service providers (ISPs) travel through these servers, where they can be filtered and possibly blocked. International internet bandwidth has increased from 318 Gbps in 2010 to 1321 Gbps in 2014.

ICT Market

The two country-level service providers offer services to licensed ISPs, which in turn sell connections to dial-up and leased-line clients. The number of ISPs in the country rose from 23 in 2005 to 36 in 2011. Broadband and mobile phone services are provided by the three largest telecommunications companies in the Middle East: Saudi Telecom Company, Mobily (owned by Etisalat of the United Arab Emirates), and Zain (from Kuwait). Two newly licensed companies have started with limited operation: Virgin Mobile in October 2014 and Lebara in December 2014.

Access to Wikipedia is provided free of charge by STC to all of its mobile data users, while Zain pro-

---

Saudi Arabia

vides unlimited access to YouTube as part of one of its prepaid mobile packages.14

Internet cafes, once prevalent, have become less popular in recent years due to the broad availability and affordability of home broadband access. Internet cafes are mainly used by youth from lower socio-economic backgrounds to congregate and socialize. Due to a mandate issued by the Ministry of Interior (MoI) on April 16, 2009,15 all internet cafes must close by midnight, with compliance enforced by the police.16 These measures were ostensibly designed to crack down on internet use by extremists, but in practice they allow the police to deter any activity that the government may find objectionable. Conversely, coffee shops have grown in popularity among business people, young adults, and single males, who enjoy free Wi-Fi access with their paid beverages.

Regulatory Bodies

Previously, all internet governance fell under the purview of the Internet Services Unit (ISU), a department of the King Abdulaziz City for Science & Technology (KACST). Established in 1998 and reporting directly to the Vice President for Scientific Research Support of KACST, the ISU now only provides internet access to government departments, as well as Saudi research and academic institutions.17 In 2003, the governmental Saudi Communication Commission was renamed to become the Communications and Information Technology Commission (CITC) and became responsible for providing internet access to the private sector, in addition to resolving conflicts among the private telecommunication companies.18 The CITC is also responsible for controlling the price that telecommunications companies are allowed to charge for cross-network calls. For example, in February 2015, the maximum charge of local voice calls between different networks was lowered.19 Furthermore, the CITC sends content removal requests to social networks in political cases (see “Content Removal” section below). The board of directors of the CITC is headed by the Minister of Communications and Information Technology.20

Limits on Content

The Saudi government continued to employ strict filtering of internet content throughout 2014 and early 2015. Self-censorship remains prevalent when discussing topics such as politics, religion, or the royal family. Nonetheless, high levels of social media use have driven an immense diversification of online content, offering Saudis a multitude of perspectives beyond state-controlled media. These tools have also been used by ordinary citizens and human rights activists to raise awareness of issues surrounding political reform, poverty, gender inequality, and corruption. However, numerous arrests and lengthy prison sentences have had an overall chilling effect on online activism.

Blocking and Filtering

Saudi Arabia

Officially, sites that are judged to contain “harmful,” “illegal,” “anti-Islamic,” or “offensive” material are routinely blocked, including pages related to pornography, gambling, and drugs. Authorities also seek to disrupt violent networks and the dissemination of extremist ideology. Criticism of the Saudi royal family or that of other Gulf Arab states is not tolerated, and neither are sites that organize political opposition or question the ruling family’s strict conception of Islam. Websites that may be used to distribute copyrighted materials, such as the Pirate Bay, are blocked. In 2014, the communications ministry blocked dozens of websites for failing to obtain an online publication license.

Websites and social media pages belonging to human rights or political organizations, such as the Saudi Civil and Political Rights Organization (ACPRA) and the Arab Network for Human Rights Information (ANHRI), are blocked. Sites belonging to several Saudi religious scholars and dissidents are blocked, as well as those related to the Shi’a religious minority, such as Rasid, Yahosein, and Awamia. Authorities also blocked the website of the Islamic Umma Party, the country’s only underground (and illegal) political party, which has called for the royal family to step down. Website mirroring is often used to circumvent blockage, but mirrors are often detected and blocked in a cat-and-mouse game. For example, authorities blocked the official website for the “October 26th Women Driving campaign” on September 29th, 2013. One week later, a mirror site was also blocked.

The CITC has also blocked individual social media pages that demand political reforms or civil rights. However, the move by many companies to standardize encrypted “HTTPS” communication has rendered much of this blockage useless, since it is technically very difficult for authorities to block individual pages on an HTTPS domain, rather than a standard HTTP domain. Authorities have occasionally moved to block entire online products and services for breaching the country’s strict laws. In September 2012, the government threatened to block all of YouTube if Google, the site’s owner, did not restrict access to the controversial “Innocence of Muslims” video containing an offensive depiction of the Prophet Mohammed. Google later blocked the video in Saudi Arabia.

The CITC also has an aggressive stance toward Voice over Internet Protocol (VoIP) services that circumvent the country’s regulatory environment and, by some indication, the surveillance apparatus. So far only Viber has been blocked, though authorities have threatened to institute further restrictions on services such as Whatsapp or Skype. BlackBerry services were temporarily stopped on June 30, 2012 following glitches experienced by the BlackBerry maker Research in Motion, according to Saudi Telecom Company (STC). There was no evidence to suggest that the government was be-
Saudi Arabia

hind the short suspension.32

The government responds to blockage requests from members of the public, who can use a web-based form to submit a complaint regarding undesirable material.33 Sites can also be unblocked through a similar process.34 Once an individual submits the form, a team of CITC employees determines whether the request is justified. In 2014, the CITC received 466,863 blockage requests, and complied in 94.3 percent of cases. Pornographic content accounted for 85.6 percent of these requests. The CITC has been developing blocking tools based on IP address, in order to prohibit websites from circumventing blockage by changing their domain name. Currently, this affects over 2,500 websites.35 The manager of public relations at the CITC said the commission receives about 200 unblocking requests each day, though he would not comment on how often the CITC unblocks a site based on such an appeal.36 In one example, the CITC unblocked the website Mustamel after the owners complied with a request from the CITC to remove illegal advertisements.37

The government is somewhat transparent about what content it blocks. While the list of banned sites is not publicly available, users who attempt to access a banned site are redirected to a page displaying the message, “Access to the requested URL is not allowed!” In addition, a green background is displayed on sites blocked by the CITC, whereas sites blocked by the Information Ministry for licensing violations or copyright infringement have a blue background. Still, a full list of banned sites is not publicly available. The country’s two data service providers must block all sites banned by the CITC,38 and failure to abide by these bans may result in a fine of up to SAR 5 million (US$1.33 million), according to Article 38 of the Telecommunication Act.39 It should be noted, however, that many Saudi internet users have become savvy at using circumvention tools such as Hotspot Shield, which allows users to access a virtual private network (VPN) to bypass censorship,40 but many other tools to circumvent blockage, such as Tor and the major VPN providers, are actively blocked by the government.41

Content Removal

Blocking and filtering are compounded by the self-censorship that online news moderators and site owners must exercise. Gatekeepers frequently delete user-generated content that could be deemed inappropriate or inconsistent with the norms of society, as they can be held legally liable for content posted on their platforms.42 This often results, for example, in keeping only progovernment user comments. It is unusual to find any antigovernment comments the websites of major Saudi newspapers, which do not reflect the diversity of political views seen on social networks.

40 Saudis refer to this circumvention tool as a “proxy breaker”
41 Examples include Hotspot Shield, Hide My Ass! and AirVPN.
Saudi Arabia

The CITC also sends requests to social networks to remove content. Facebook’s Government Requests Report of the first half of 2014 cites 7 processed requests that were “reported by the Communications and Information Technology Commission (CITC) under local laws prohibiting criticism of the royal family.” On the other hand, Twitter reported no content removal requests from Saudi Arabia in the period from 2012 to 2015.

Copyright takedown requests were also used to restrict political speech. In September 2014, an episode of a satirical show on YouTube called *Fitnah* was censored when the Saudi TV channel, Rotana sent a Digital Millennium Copyright Act (DMCA) notice to take it down. The show used footage from the channel to criticize its owner, Prince Waleed Bin Talal, who was accused by the show of being responsible for the takedown request. The video was later restored.

**Media, Diversity, and Content Manipulation**

Social media users are increasingly careful about what they post, share, or “like” online, particularly after the passage of a new antiterrorism law in 2014. Users who express support for extremism, liberal ideals, minority rights, or political reforms, in addition to those who expose human rights violations, are closely monitored and often targeted by the government. Questioning religious doctrine is strictly taboo, particularly content related to the prophet Mohammed. Influential Twitter users, such as Essam al-Zamil, are growingly fearful of expressing support for outspoken activists who have been recently sentenced to jail time. Others have decided to leave Twitter. Government consultants have stopped contributing to foreign newspapers due to pressure from other government agency representatives.

With so much activity occurring on social networks, the Saudi government maintains an active presence online as a means of creating the illusion of popular support for its policies. It is believed the government employs an “electronic army” to constantly post progovernment views, particularly on social media. Progovernment trolls have taken to “hashtag poisoning,” a method of spamming a popular hashtag in order to disrupt criticism or other unwanted conversations through a flood of unrelated or opposing tweets. Through the use of a “bot,” such as those provided by Yoono.com, one individual can send thousands of tweets to a hashtag at the same time. While the tweet may contain the same message, the bot sends the tweet on behalf of numerous fabricated accounts, created by combining random photos of faces with names culled from the internet. The government also influences online news reporting by offering financial support to news sites such as Sabq and Elaph in return for coordination between site editors and the authorities. Individuals may also be awarded upon praising the government online. In April 2015, the MoI awarded eight young people who had published a video responding to threats from the IS militant group with progovernment support.

---

Saudi Arabia

rhetoric. The speaker was awarded 100,000 SAR (US$26,600), and those sitting with him were awarded 50,000 SAR (US$13,300).50

Whereas the authorities provide monetary support to progovernment websites, the owners of opposition websites can come under strong financial pressures as a result of the country’s environment of censorship. Revenue from third-party advertisers can be heavily impacted by a government decision to block a website. The government can also request advertisers cancel their ads on a particular website in order to pressure the website to close. Restrictions on foreign funding further inhibit the sustainability of websites that are critical of the ruling system. Numerous sites have been closed for copyright violations,51 or for featuring advertisements for drugs.52

While opposition blogs and online forums were once the main venue for discussing political and social matters, most Saudis now use social media to share information and express opinions. There are now dozens of comedic channels on YouTube, the most popular being “Sa7i,” “Eysh Elly,” “La Yekthar,” and “3al6ayer,” which respectively had around 351 million, 276 million, 85 million, and 68 million total views as of 2014. Omar Hussein, host of 3al6ayer, has touched on political issues and come out in support of a woman’s right to drive. On Eysh Elly, Badr Saleh compiles and makes fun of popular Saudi YouTube videos.53 One reason for the success of these videos is their engagement in cautious criticism and their restraint against pushing the limits of acceptable discourse. Saudi companies such as C3 (Creative Culture Catalyst) and Jeddah-based UTURN have sprung up to provide funding and support for video production in the kingdom, with great success. Opposition figures overseas use YouTube as a platform for distributing their audio and video content, since their websites are blocked within the country.54

Similarly, Saudis are the largest adopters of Twitter in the Arab world, according to a 2014 report, with 4.8 million users55 and producing 40 percent of all tweets in Arab countries.56 Prominent religious scholars, such as al-Awdah, have even contributed to these debates on Twitter.57

Digital Activism

Saudis have employed online tools for holding government officials accountable, mainly through the use of smartphones to capture videos of corruption or improper behavior. On April 7, 2015, the Minister of Health was filmed shouting at another citizen during a heated argument58 and was dismissed four days later. In May 2015, the head of the Royal Ceremonies office was recorded slapping a journalist who was trying to cover the reception of the king of Morocco, and was also dismissed.59

54 Examples include Sa’ad Al-Faqih, Mohammad al-Massari and Mohammad al-Mofarreh.
59 “In video....For that Mohammad al-Tubushi, Head of Royal Ceremonies, was dismissed,” Al Arabiya, May 5, 2015, https://bit.ly/1Tc9zaM.
media took both cases as gestures of the new king’s intolerance for public officials’ moves to offend the “dignity” of citizens.60

The campaign to defy the ban on women driving was less successful this year.61 Before the first anniversary of the October 26 Campaign, the spokesperson of the MoI threatened that the ministry would be “firm in enforcing the regulations against anyone who tries by any means to damage the societal harmony by spreading what splits and polarizes the society,” in reference to calls for women driving.62 This was followed by increased police presence on the day of the anniversary, and only a few videos were uploaded to YouTube showing women defying the ban.

The anonymous Twitter user @Mujtahidd continues to criticize high profile members of the royal family,63 and to provide detailed descriptions of state corruption.64 The popularity of the account has increased more than four times, from around 410,000 Twitter followers in June 2012 to over 1.8 million as of June 2015. In 2013, the user shared the tweets of dozens of users who defended the government using the exact same wording, thus illustrating the presence of a MoI Twitter army.65 In March 2015, the account was suspended several times over the course of two days, but was reinstated without explanation.

The efficacy of security forces in dispersing public demonstrations has forced many Saudis to devise more creative ways of organizing protests. Two Twitter accounts, in particular @e3teqal and @almnaseron, played a major role in organizing small, distributed, low-level protests during 2012 and 2013 with anonymous participants who were sympathetic to political prisoners and imprisoned religious scholars. YouTube was instrumental in documenting the demonstrations and attracting media attention.66 Videos documented a protest on June 6, 2012, in which a group of detainees’ families carried out a demonstration inside a shopping mall after initially pretending to be regular customers.67 Later that summer, demonstrators “marched” together in their cars on a highway.68 In March 2013, 182 family members, including 15 women and 6 children, participated in a 12-hour sit-in in the central city of Buraidah. Police arrested 161 of the protestors and blamed social media for stirring up the protests.69 More recently, however, with the increased crackdown on protesters, these accounts have failed to gather momentum.

62 “MoI: Regulations will be enforced against anyone that contributed to what allows the ill-intended to disturb societal harmony and polarizes society,” [in Arabic], Okaz, October 23, 2014, http://www.okaz.com.sa/24x7/articles/20141023/article20725.html.
63 Worth,”Twitter Gives Saudi Arabia a Revolution of Its Own.”
66 “Petitioning the Saudi government King Abdullah Al-Saud: Free Tariq Al-Mubarak,” http://chn.ge/1VNrVPJ.
Saudi Arabia

Violations of User Rights

Saudi courts have delivered some of the harshest prison sentences against online users in the world, with numerous human rights defenders jailed for periods of 10 to 15 years for their online activities. The legal environment surrounding online expression remains a significant impediment to internet freedom, and it has only worsened over the past year. The 2014 antiterrorism law, which equates “insulting the reputation of the state” with terrorism, was used to prosecute peaceful activists. Furthermore, as legal limits on the detention of suspects were removed, numerous Saudis are now legally detained for periods of months—and sometimes years—without charge.

Legal Environment

Saudi Arabia has no constitution. The Basic Law of Saudi Arabia contains language that calls for freedom of speech and freedom of the press, but only within certain boundaries. The 2000 Law of Print and Press also addresses freedom of expression issues, though it largely consists of restrictions on speech rather than protections. Online journalists employed at newspapers and other formal news outlets maintain the same rights and protections as print and broadcast journalists, and like their counterparts, are also subject to close government supervision. Similarly, laws designed to protect users from cybercrimes also contain clauses that limit freedom of expression. The 2007 Anti-Cyber Crime Law criminalizes “producing something that harms public order, religious values, public morals, the sanctity of private life, or authoring, sending, or storing it via an information network,” and imposes penalties of up to five years in prison and a fine of up to SAR three million (US$800,000).70

The antiterrorism law, passed in January 2014, defines terrorism in such vague terms that nonviolent acts, such as “insulting the reputation of the state,” “harming public order,” or “shaking the security of the state,” are criminalized as applicable offenses.71 Article 1 of the law defines “calling for atheist thought in any form” as terrorism.72 Article 4 prohibits support for banned groups by “circulating their contents in any form, or using slogans of these groups and currents [of thought], or any symbols which point to support or sympathy with them” through audio, visual, or written format, including websites and social media.73

Prosecutions and Detentions for Online Activities

Saudi Arabia’s restrictive laws have been rigorously applied to silence critical voices and human rights defenders. Since traditional political organizing is banned in the country, many human rights activists conduct activities online given the reach of social media tools in the country. As a result, the authorities often prosecute activists for setting up websites, posting on Twitter, or appearing in YouTube videos documenting human rights abuses or calling for government action. For example, in December 2014, Loujain al-Hathloul was arrested at the border crossing between Saudi Arabia and the United Arab Emirates when she demanded to be allowed to drive in Saudi Arabia. She was referred to the Specialized Criminal Court, a terrorism tribunal, on charges related to political opinions

she had expressed on Twitter and other social media sites and was held in detention for 73 days. In July 2014, well-known human rights lawyer Waleed Abu al-Khair was sentenced to 15 years in prison by the Specialized Criminal Court. Abu al-Khair was targeted for his nonviolent activism, including statements he made on Twitter and various media outlets related to the government’s detention of prisoners of conscience. He had been arrested in April on numerous charges including “disobeying the ruler,” “disrespecting the authorities,” “offending the judiciary,” “inciting international organizations against the Kingdom,” “founding an unlicensed organization,” and violating the cybercrime law. He is the head of the organization “Monitor of Human Rights in Saudi Arabia” and the husband of Raif Badawi’s sister, human rights activist Samar Badawi. He was also banned from travel from 15 years after release and fined SAR 200,000 (US$53,000). Originally, five years of his prison sentence were suspended, but after an appeal by the prosecution in January 2015, the court ruled Abu al-Khair must serve all 15 years.

Similarly, following an appeal from the public prosecutor, Fowzan al-Harbi was sentenced to 10 years in prison in November 2014, including a 10-year travel ban upon release. He had been detained in December 2013 on charges of “inciting disobedience to the ruler by calling for demonstrations,” “describing the Saudi Arabian state as a ‘police state’,” “accusing the judiciary of being incapable of delivering justice,” “signing documents that incite public opinion against the authorities,” as well as charges related to his co-founding of the human rights organization ACPRA. Al-Harbi was sentenced to seven years in prison in June 2014 but was released pending an appeal after signing a pledge to refrain from using social media and socializing with others. However, he was accused of later publishing the charges against him online in a violation of the terms of his release, leading to his immediate arrest and the increased sentence.

A court in Riyadh disbanded the ACPRA in March 2013 and sentenced two of its members, Abdullah al-Hamid and Mohammed al-Qahtani, to 11 years and 10 years of jail time respectively, in addition to a travel ban equal in length to their jail sentences. Five years of their sentences were based on Article 6 of the Anti-Cyber Crime Law, relating to the creation of a website that could disturb social order. Six founding members of ACPRA are currently in detention. Two founding members of the Islamic Umma Party, al-Wahiby and al-Gamidi, have been in prison since February 2011. Both the

---

83 Those members are Sulaiman Al-Rushoodiy, Mansour Al-Awth, Mousa Al-Garni, Mohamed Al-Bijadi, Saleh Al-Ashwan and Fawzan Al-Harbi.
Saudi Arabia

ACPRA and the Islamic Umma Party base many of their operations online.

Raif Badawi, the co-founder of the Saudi Arabia Liberals website who has been imprisoned since June 2012, had his sentence increased from 7 to 10 years in jail and from 600 to 1,000 public lashes, as well as a fine of SAR one million (US$266,000) in early May 2014. Badawi was charged with "setting up a website that undermines general security" and "ridiculing Islamic religious figures." On January 9, 2015, Badawi received 50 lashings outside a mosque in Jeddah, following Friday prayer. Footage of the punishment was uploaded to YouTube, resulting in a massive international backlash. Further lashings have been postponed. In February 2015, the sentence was suspended by the Supreme Court to be reevaluated, but later in June, the court upheld the verdict.

Several others were arrested for criticizing the state-sponsored religious institution. On October 28, 2014, Su’ad al-Shammari, co-founder of the Saudi Arabia Liberals website, was arrested over tweets that were described as offensive to the heritage of the prophet Mohammad. She was released on February 1, 2015 after signing a pledge to “reduce her activity”. Her Twitter account, however, is still critical of the religious institution. In late January 2015, Waheed al-Ghamdi was arrested over a series of articles in which he addressed sectarianism by blaming the same religious body. He was released on March 2, 2015, after his case was assigned to the Ministry of Culture and Information.

In April 2015, the Specialized Criminal Court sentenced a Saudi citizen from Riyadh to a year and four months in prison and a travel ban for three years for participating in protests that called for the release of the arbitrarily detained, for storing audio and video clips of protests on his computer, and for uploading them to YouTube. The court also ordered the closure of the citizen’s social media and email accounts, a common practice in Saudi Arabia. Another citizen, this time from Qatif, was sentenced by the same court in December 2014 to five years in prison for charges that included “creating nicknames on the social media websites Twitter and Facebook, and using them to publish forbidden articles”.

While there were numerous cases of sentences being extended upon appeal, in at least one case, charges were dropped. In April 2015, the Court of Appeals overturned five to eight year prison sentences against three lawyers—Abdel Rahman al-Subehi, Bander al-Nakithan, and Abdel-Rahman al-Remaih—who were convicted of “insulting” and “interfering with the purview” of the ruler and the

Saudi Arabia

judiciary in October 2014 after criticizing the slow pace of judicial reform on Twitter.

Surveillance, Privacy, and Anonymity

Surveillance is rampant in Saudi Arabia; anyone who uses communication technology is subject to government monitoring, which is officially justified under the pretense of protecting national security and maintaining social order. The authorities regularly monitor websites, blogs, chat rooms, social media sites, emails and mobile phone text messages. Evidencing the government’s determination to monitor its citizens, the American security expert Moxie Marlinspike published email correspondence with an employee at Mobily who sought to recruit him to help the telecommunications firm intercept encrypted data from mobile applications such as Twitter, Viber, Vine, and WhatsApp.

According to a report from the University of Toronto’s Citizen Lab, the government has coordinated with the company Hacking Team in order to target Saudis in the region of Qatif with surveillance malware. A legitimate news app titled Qatif Today, available to Android mobile devices through the Google Play store, was manipulated in order to spy on users with an interest in the Saudi region of Qatif, which has undergone numerous protests. A link circulated on Twitter directed users to a Dropbox file that downloaded the phony app developed by Hacking Team, an Italian company that sells intelligence products to governments. Among other things, the app appeared to be designed to grant authorities access to individuals’ mobile phone data, social network activity, as well as real-time recording capabilities using the phone’s microphone and camera.

New registration requirements have undermined the ability to use ICT tools anonymously and free from government interference. The Ministry of Culture and Information requires that all blogs, forums, chat rooms, and other sites obtain a license from the ministry to operate, thus putting more pressure on online writers to self-regulate their content. However, this rule is enforced only on popular online publications. Even anonymous users and writers who employ pseudonyms when making controversial remarks face special scrutiny from the authorities, who attempt to identify and detain them.

Users are legally required to use their real names and register with the government when purchasing mobile phones. In 2012, the CITC introduced a new law making it mandatory to enter a user’s ID number to recharge a prepaid mobile card, rendering it virtually impossible to use prepaid mobile phones anonymously. Nevertheless, a black market has since emerged in which vendors sell new SIM cards and prepaid refill cards with pre-existing ID numbers. To stop this lucrative practice, the government is now considering linking these cards to fingerprints.

In addition to direct government monitoring, access providers are required to monitor their own customers and supply the authorities with information about their online activities, often without

due process. Since 2009, the MoI has made it mandatory for internet cafes to install hidden cameras and provide identity records of their customers. The security regulations also bar entrance to anyone under the age of 18.

**Intimidation and Violence**

Most gravely, in May 2015, political activist Waleed Sulais was beaten during a funeral for the victims of an IS attack on a Shiite mosque. Two men accused Sulais of insulting them on social networks, and physically assaulted him. The attackers were also Shiites, and had been wanted by the authorities.105

Progovernment Twitter accounts often defame and harass political and social activists using hashtags calling for their arrest. The anonymous accounts often show photos of the king or the interior minister as their avatars. In March 2014, the Ministry of Interior released a list of organizations classified as “terrorists,” which included the Muslim Brotherhood. Following that, the MoI contacted influential Twitter users containing the “Raba’a” logo in their avatar and ordered them to remove it; the logo refers to the square in which anti-coup protesters in Cairo held their sit-in, before a violent crackdown by the Egyptian army in August 2013. Those who refused were called in for interrogation and ordered to stop using their Twitter accounts.106

**Technical Attacks**

In April 2015, during the Saudi-led war against Houthi militants in Yemen, a group of Houthi supporters called the “Yemen Cyber Army” hacked into the website of Saudi-sponsored newspaper al-Hayat, displaying the photo of Hezbollah Secretary General Hassan Nasrallah and writing in Arabic: “We have few words to say to you, prepare your bomb shelters.”107 In May 2015, the same group attacked the mail service of the Foreign Ministry publishing thousands of email correspondences, claiming they were “top-secret.”108 The Ministry claimed that the attack was “limited.”109

---

Singapore

Key Developments: June 2014 – May 2015

- A political website was ordered to be shut down in the first ever use of the government’s 19-year-old licensing powers (see Content Removal).

- A new anti-harassment law, ostensibly introduced to protect ordinary citizens, was wielded against critics of the government (see Prosecutions and Detentions for Online Activities).

- Three individuals were charged under the Sedition Act for postings allegedly promoting ill-will between Singaporeans and immigrants (see Prosecutions and Detentions for Online Activities).

- The prime minister sued an activist blogger, the first time a government leader has taken an individual to court for defamation over a blog post (see Prosecutions and Detentions for Online Activities).

- A prominent blogger was fined SGD$8,000 (US$5,800) for contempt of court (see Prosecutions and Detentions for Online Activities).

- A teenager was found guilty of penal code violations over an online tirade against the late Premier Lee Kuan Yew (see Prosecutions and Detentions for Online Activities).
Singapore

Introduction

Singapore entered its 21st year of public internet access in 2015. Digital connectivity has grown quickly, with the People’s Action Party (PAP) government embracing the internet as essential infrastructure for economic development. However, it remains wary of the technology’s potential for liberalizing political debate and enhancing democratic participation.

The government acknowledged that Singapore’s political culture became more disputatious after the 2011 general election. While it responded swiftly to address public grievances over various social and economic policies, it has not opened up space for dissenting views. It appears determined to contain public debate within what it considers to be acceptable boundaries.

Indeed, during preparations for the elections in late 2015, the government showed heightened sensitivity toward online dissent, resulting in a series of unprecedented actions during the coverage period. It ordered the shutdown of a highly critical political website, marking the first time that a site’s license has been suspended. A new anti-harassment law, originally touted as a means of protecting ordinary citizens from cyber stalking and other social ills, was almost immediately wielded by the government itself against its critics. Another first was the prime minister’s defamation suit against an activist blogger.

The website shutdown and the charging of three individuals under the Sedition Act were all associated with expression that the authorities claimed could inflame relations between locals and immigrants. The interventions were symptomatic of the government’s struggle to manage the highly charged debate over its unpopular immigration policies. The debate has been most vociferous online.

The government’s restrictions on online debate have not been severe enough to neutralize the internet’s importance as a space for alternative and more authentic voices. Antigovernment views are routine in comment spaces, forums, and social media.

However, the government may succeed in slowing down the growth of independent news sites and in discouraging more organized activism. Since 2013, the government has used registration and fundraising regulations to stymie the emergence of professionally-run, independent online news organizations with the capacity for original daily reporting and regular investigative journalism – of which none exist in Singapore.

Although there was much international speculation over whether the death of founding Prime Minister Lee Kuan Yew in March 2015 would usher in more political openness, there is no sign that this will be the case. On the contrary, the outpouring of sentiment over Lee’s passing may have solidified Singapore’s conservative base, strengthening the hand of hardliners who argue that Singaporeans value good governance more than civil liberties.

Obstacles to Access

As a wealthy and compact city-state, Singapore has highly developed information and communication technology (ICT) infrastructure. Its Intelligent Nation 2015 master plan for an ultra-high-speed, pervasive network achieved the target of 90 percent home broadband penetration. A new government program launched in September 2014 offers affordable broadband packages to low-income households. In
Singapore

addition, the national wireless network offers free public access. In late 2014, the government launched a high-level Smart Nation program that will include education and training to boost Singaporeans’ skills in developing digital technologies and applications.

Availability and Ease of Access

Eighty-two percent of households had internet access in 2014, while mobile phone subscriptions outnumbered residents by 58 percent.1 The fiber-based Next Generation Nationwide Broadband Network (Next Gen NBN) reached 95 percent of homes and businesses by July 2013.2 Home owners are offered free installation for the first 15 meters of fiber running into their homes. In addition, the national wireless network offers free public access.

Singapore’s Intelligent Nation 2015 master plan, its sixth consecutive masterplan for the sector, achieved the target of rolling out broadband connections to 90 percent of homes; smartphone penetration has reached 85 percent.3 In November 2014, the government launched its next major thrust, called Smart Nation, to integrate technologies more seamlessly and improve Singaporeans’ skills in not just using but also creating new technologies. A Smart Nation Programme Office has been set up under the Prime Minister’s Office, to take a “whole-of-Government, whole-of-nation approach.”4

The digital divide cuts mainly along generational lines. While close to 100 percent of residents aged 7 to 34 reported in 2012 that they had used the internet in the past year, the percentage was 51 percent for those in their 50s and 16 percent for those 60 and older.5 In September 2014, the government launched a Home Access program under its SGD 8 million (US$5.7 million) Digital Inclusion Fund, to make internet connectivity more accessible and affordable to lower-income Singaporeans. Eligible households are provided home internet access and phone services with a broadband package at SGD 6 (US$ 4.30) per month for 48 months. This includes fiber connectivity and a basic device such as a tablet.6

Restrictions on Connectivity

No known restrictions have been placed on ICT connectivity or access to social media or communication apps, either permanently or during specific events. The Singapore Internet Exchange (SGIX), a not-for-profit established by the IDA in 2009, provides an open, neutral and self-regulated central point for service providers to exchange traffic with one another directly instead of routing through international carriers, thus improving latency and increasing resiliency when there are cable outages on the international network.7

Singapore has adopted a National Broadband Network (NBN) structure, with the network built and operated by an entity that supplies telecommunications services on a wholesale-only, open-access basis.

---

4 IDA, “Transcript of Prime Minister Lee Hsien Loong.”
Singapore

and non-discriminatory basis to all telecommunications carriers and service providers. To develop Singapore’s all-fiber Next Generation NBN, a structurally separated network company has responsibility for the passive infrastructure, including the optical fiber. An operationally separate operating company is responsible for the active infrastructure, including routers, switches and access network equipment. These are in turn supposed to be separate from the retail service providers downstream, to avoid conflicts of interest. However, OpenNet, the builder-operator of the passive infrastructure, is currently controlled by a unit of government-linked Singapore Telecom (SingTel). Due to other players’ concerns that the acquisition was anticompetitive, regulators required that SingTel sell off 75 percent of its stake in that unit by April 2018.

ICT Market

The dominant internet access providers are also the mobile telephony providers: SingTel, Starhub, and M1. SingTel, formerly a state telecom monopoly and now majority owned by the government’s investment arm, has a controlling stake in Starhub. The market is open to independent entrants. One of them, MyRepublic, rolled out a lower-cost 1 Gbps broadband service in early 2014 and announced its intention to bid for a 4G license that would make it the country’s fourth telco. In March 2015, another newer player, ViewQwest, launched a 2 Gbps fiber-optic broadband service for households, offering what was touted to be among the world’s fastest home broadband plans.

Regulatory Bodies

The internet infrastructure is regulated by the Infocomm Development Authority (IDA). As a statutory body of the Ministry of Communications and Information (MCI), it takes instruction from the cabinet. In planning the all-fiber Next Gen NBN, the IDA has promised a competitive industry structure that would avoid conflicts of interest and allow retail service providers that offer services to end-users to purchase bandwidth connectivity at nondiscriminatory and nonexclusive prices.

Limits on Content

The government has kept a 1996 promise not to block or filter any political content. However, in May 2015, it took the unprecedented step of ordering a political website to shut down, on the grounds that it had violated the Internet Code of Practice. A licensing system introduced in 2013 has been used to limit the growth of independent online news start-ups by restricting their funding options. Also in operation are powers to issue takedown orders to large commercial online news media. Despite these limits, the internet remains significantly more open than print or broadcasting as a medium for news and

---

Singapore

political discourse, which flow online largely unhindered. Restraints in online discourse are mainly due to fear of post-publication punitive action—especially through strict laws on defamation, racial and religious insult, and contempt of court (see Legal Environment).

Blocking and Filtering

The Broadcasting Act has included explicit internet regulations since 1996. Internet content providers and internet service providers (ISPs) are licensed as a class and must comply with the act’s Class License Conditions and the Internet Code of Practice. Under this regime, ISPs are required to take “all reasonable steps” to filter any content that the Media Development Authority (MDA) deems “undesirable, harmful or obscene.”

As a matter of policy, the MDA blocks only a list of 100 websites, for the purpose of signposting societal values. This floating list has never been made public, but no political site has been blocked. Other than a few overseas sites run by religious extremists, the list is known to comprise pornographic sites. Outside of this list, the Canada-based extramarital dating website, Ashley Madison, has been blocked since 2013, after it announced its plan to launch in Singapore. No other site was subsequently singled out for similarly targeted blocking. The use of regulation to signpost social values has been linked to the influence of religious conservatives (mainly evangelical Christians) asserting themselves more in public morality debates.

Like the IDA, the MDA is a statutory MCI body and answers to the cabinet. The Broadcasting Act empowers the MCI minister to prohibit disclosure of any directions to censor content. This—together with the fact that most ISPs and large online media companies are close to the government—results in a lack of transparency and public accountability surrounding online content regulation.

Content Removal

In May 2015, the MDA declared that The Real Singapore (TRS) website had violated the Internet Code of Practice, and that its Class License was therefore suspended. Its owners were required to disable access to the website. They have apparently complied: visitors to the site now see the message, “The Real Singapore has been ordered to disable access to all our online services by the Media Development Authority (MDA) of Singapore.” This was the first time since the Class License system was introduced in 1996 that such action has been taken. A local network of digital freedom activists, FreeMyInternet, criticized the MDA’s action as “arbitrary and unsubstantiated,” and indicative of “disproportionate power vested in a statutory board, and unclear guidelines on actions to be taken against objectionable content.”

17 Broadcasting Act (Chapter 28) Section 3(5).
Singapore

The MDA said that the TRS had “published prohibited material as defined by the Code to be objectionable on the grounds of public interest, public order and national harmony.” It did not specify what content had crossed the line, but said that several articles had “sought to incite anti-foreigner sentiments in Singapore.” Some articles were “deliberately fabricated” and “falsely attributed.” It said that TRS, previously run from outside of the country, came within the jurisdiction of the Broadcasting Act in December 2014, when two of the editors arrived in Singapore. The editors were given six hours to disable access to its site, and seven days to present arguments as to why their class license should not be cancelled. The two editors were also charged with sedition (see Prosecutions and Detentions for Online Activities).

The information minister said that this was only the 27th intervention against online content since 1996, and the first time a site had been shut down. Previous cases apparently involved takedown notices for specific content. These are not made public. However, in 2013, the minister informed parliament that most takedowns were for pornographic content or solicitation; others were related to gambling or drugs. He told parliament that the MDA had never directed websites to take down content “just because it is critical of the Government.”

A separate notice-and-takedown framework exists for large online news sites. Introduced in June 2013, it removes the identified sites from the class license and subjects them to individual licensing, under which they are required to comply with any takedown notice within 24 hours. The sites are required to put up a “performance bond” of SGD 50,000 (US$35,600) as an incentive to exercise best efforts. The bond is in line with the requirement for television niche broadcasters.

Ten news sites were on the initial list to be licensed under the new framework. Nine are run by Singapore Press Holdings or MediaCorp—which, as newspaper and broadcasting companies, are already subject to discretionary individual licensing and traditionally cooperate with the government. The new regulation was probably prompted by Yahoo Singapore’s news site, the only one of the ten not belonging to national mainstream media. However, although occasionally slightly bolder in its political coverage, neither it nor the other nine sites were likely to disobey a takedown request even without the new regulations. After it was licensed, Yahoo’s reporters were granted the official accreditation that they had sought for several years.

Although the government said the operations of the licensed sites would be virtually unaffected, the new framework raised concerns about the transparency and independence of regulation. The new licensing framework was made public through a press release three days before it was implemented. Formally, the framework covers sites reporting an average of one article on Singapore’s news and current affairs per week over a continuous two-month period, and receiving visits from a monthly average of 50,000 unique IP addresses from Singapore over those two months. However, bloggers and other observers said that the criteria were unclear and inconsistently applied. The government’s assurances that commentary-driven blogs would not be subject to the new framework were not

Singapore

written into the regulations and only deepened unease about their arbitrary application. In July 2015, outside the coverage period of this report, two independent sites, Mothership.sg and Middle Ground, were subject to the same framework.

Several bloggers have publicly acknowledged removing critical content under threat of criminal prosecution or defamation suits (see Prosecutions and Detentions for Online Activities), while others are widely believed to do the same behind the scenes.

Media, Diversity, and Content Manipulation

Singapore’s highly targeted regulations have an impact on the diversity of its online landscape, both within the mainstream media sector as well as alternative media and blogs. The biggest online news players, in terms of resources and viewership, are the internet platforms of the mainstream newspaper and broadcast outlets of Singapore Press Holdings (SPH) and MediaCorp. They are subjected to the new notice-and-takedown framework, but the main avenue of control is the routine self-censorship that also afflicts their parent news organizations. MediaCorp is 80 percent government-owned, with SPH holding the remaining 20 percent. SPH is a listed company, but through the Newspaper and Printing Presses Act, the government can nominate individuals to its board of directors. Since the 1980s, every SPH chairman has been a former cabinet minister. The government is known to have a say in the appointment of chief executives and chief editors. It also wields significant powers of patronage. Compared with authoritarian regimes that are more fractured and offer alternative sources of elite support, power and influence in Singapore are unusually centralized within the PAP's top echelons.

For all these reasons, news websites run by mainstream media tend not to deviate significantly from the official line on controversial political issues, even in their opinion columns. While self-censorship is inherently difficult to monitor, bloggers have found evidence that mainstream news websites edited potentially contentious articles. In 2015, the SPH-owned national daily Straits Times deleted an online report quoting a cabinet minister, apparently because his comments were backfiring on the government. MediaCorp’s Channel NewsAsia online portal deleted a report on a public forum after a junior minister’s answer to a question about national servicemen’s pay proved controversial. What was striking about these two cases is that they went beyond the expected downplaying of dissenting views, and involved manipulation of factual news reports on officials’ own public statements. This may be indicative of the extreme sensitivity to potential controversies in the run-up to the late 2015 election.

Given the constraints that mainstream media work under, independent online media add significantly to the diversity of content. However, most socio-political blogs generate negligible revenue and therefore lack the manpower to generate original reporting and commentary on a daily basis. Efforts to professionalize citizen media have been hamstrung by government regulations introduced in 2013, which targeted smaller start-ups with ambitions to go commercial. On a case by case basis, publishers are required to sign an undertaking not to receive funds from foreign sources other than

27 Belmont Lay and Jonathan Lim, "The Straits Times censors Minister Chan Chun Sing’s ‘tikam’ & ‘enjoy a windfall’ quotes about Pinnacle@Duxton,” Mothership, February 26, 2015, http://bit.ly/18XInK8;
Singapore

commercial advertising and subscription revenue. In addition, each has had to submit to the MDA detailed personal information about its owner, editorial team, and source of funds, including the names and national identity card numbers of individual funders.29 These conditions were applied to three sites in 2013 and early 2014; as a result, one voluntarily closed down. In September 2014, the conditions were once again applied to a new company, The Opinion Collaborative, which was set up to run the leading independent site, The Online Citizen. The company complied with the request.

Although a registration system for political and religious sites had been in place since the 1990s, the earlier version did not impose any restrictions on their operations. The revised registration process, with its ban on foreign funding, appears designed to close off the possibility of any Singaporean site replicating the formula of independent news website Malaysiakini across the border in Malaysia. Malaysiakini had received startup grants and loans from overseas before becoming commercially viable. The websites that the government targeted with its new registration rules were not the most radical in Singapore’s cyberspace, but stood out for wanting to place citizen journalism on a financially sustainable footing.

While the government may have succeeded in inhibiting the growth of more professional and organized online journalism, the more informal sector remains vibrant. YouTube, Facebook, Twitter, and international blog-hosting services are freely available, and most bloggers are able to operate openly. In addition to sites devoted to politics and current affairs, there are several NGO sites contributing to debates within their respective spheres, such as TWC2 (promoting migrant worker rights) and Transitioning (opposing the PAP’s immigration policies).30

All major opposition parties are active online. Social media discourse remains disproportionately critical of the government. Since the 2011 election, individual ministers and government agencies have ramped up and professionalized their social media capacity. Major government campaigns regularly and openly commission bloggers and creative professionals who are not ideologically opposed to such relationships. There is no evidence of large scale deployment of cyber troops. However, PAP supporters appear to be shedding some of their former reticence and, encouraged by their leaders’ example, are expressing themselves more, especially on Facebook. The government's efforts to increase its internet presence through websites like Factually31 and FiveStarsAndAMoon32 have at most narrowed the gap with its critics. It has not been able to extend its unfair offline advantage into the online space.

Digital Activism

The internet is regularly used for popular mobilization, the success of which is constrained less by online regulation than by offline restrictions on fundraising and public assembly.

Online activism played a role in voicing public discontent over the government’s pension system, the Central Provident Fund (CPF). Activists who believe that the CPF lacked transparency and flexibility held a series of “Return Our CPF” protests at Hong Lim Park. The protest numbers appeared to have

Singapore

been buoyed by the controversy over the Prime Minister’s defamation suit against activist-blogger Roy Ngerng, who was one of the central figures in the protest movement (see Prosecutions and Detentions for Online Activities).33 Addressing public disquiet, the government moved to make CPF withdrawal rules more flexible. However, the government did not provide the level of transparency that critics had demanded.34

Another online campaign centered upon a controversial relationship workshop for junior college students run by Focus on the Family Singapore, a Christian group. A junior college student publicized the workshop and its contents on Facebook, and the post eventually went viral, with many questioning the gender stereotypes in the workshop’s content. The junior college eventually did not renew the workshop for its students.35

Online activism was a major feature in the ongoing debate over LGBTI rights. The LGBTI community’s annual Pink Dot gathering on June 28, 2014 drew a record 26,000 participants, largely mobilized online.36 The event also attracted a counter-campaign by different religious groups. A group of Muslims launched an online campaign to wear white to protest the LGBTI movement’s perceived threat to family values. They also took offense to Pink Dot being held on the first day of the holy month of Ramadan.37 The largest Wear White gathering comprised 6,000 worshippers at the Faith Community Baptist Church.38

Violations of User Rights

While citizens remain free from major human rights abuses and enjoy high levels of personal security in Singapore, the government places a premium on order and stability at the expense of civil liberties and political opposition. During the coverage period, the prime minister won a defamation lawsuit against a blogger, while another blogger was convicted on a contempt of court charge. A teenager who posted a political tirade was convicted for obscenity and for wounding religious feelings. Three individuals were charged under the Sedition Act. A website and a blogger were charged under the new anti-harassment law. The authorities are believed to exercise broad legal powers to obtain personal data for surveillance purposes in national security investigations.

Legal Environment

The republic’s constitution enshrines freedom of expression, but also allows parliament wide leeway to impose limits on that freedom.39 As the ruling party has consistently controlled more than 90 percent of seats in the legislature, laws passed tend to be short on checks and balances. The Newspaper

and Printing Presses Act and the Broadcasting Act, which also covers the internet, grant sweeping powers to ministers, as well as significant scope for the administrative branch to fill in the details through vaguely articulated subsidiary regulations, such as the website licensing and registration rules described earlier in this report (see Limits on Content). Other laws that have been used against online communication, such as the Sedition Act and Political Donations Act, are open to broad interpretation by the authorities.

The Sedition Act, dating from colonial times, makes it an offense “to bring into hatred or contempt or to excite disaffection against the Government” or “to promote feelings of ill-will and hostility between different races or classes of the population of Singapore,” among other things. Punishments for first-time offenders could include a jail term of up to three years. Newer provisions in the penal code (Section 298) provide for jail terms of up to three years for offenders who act through any medium with the “deliberate intention of wounding the religious or racial feelings of any person.” Singapore’s first cases of imprisonment for online speech were under the Sedition Act in 2005, over postings insulting Muslims. This was also the first prosecution under the Sedition Act since independence in 1965. One of the side effects of Singaporeans’ participation in social media, bypassing experienced mainstream media gatekeepers, is that members of the public now have more opportunities to give and take racial or religious offense through content posted online. Police investigations into complaints of insult and offense appear to be a regular occurrence. In most known cases, police intervention at an early stage has been enough to elicit apologies that satisfy those who feel targeted by offending expression. Occasionally, however, charges are brought against the offenders.

Defamation is criminalized in the penal code, but to date, no charges have been brought under this law to punish online speech. Civil defamation law is fearsome enough. PAP leaders have been awarded damages in the range of SGD 100,000 to 300,000 each (US$71,000 to US$213,000) in defamation suits brought against opposition politicians and foreign media corporations. Electronic media have been affected: in 2002, a libel suit was leveled at Bloomberg for an online column; it settled out of court and paid three leaders damages totaling SGD 595,000 (US$422,000). The government has not heeded recommendations by international human rights groups to introduce caps on compensation for nonmaterial harm to reputation. There has also been no move to modernize Singapore’s plaintiff-friendly defamation law in line with recent developments in British and other Commonwealth jurisdictions, which have sought to safeguard legitimate political debate in the broader public interest. Similarly, the offense of scandalizing the judiciary has been used in Singapore to punish criticism of the court that in most democracies would be considered to fall within the norms of political debate. In 2008, a blogger was sentenced to three months in prison for this offense.

In April 2014, a new Protection from Harassment Act came into force. It was touted by the govern-

40 Sedition Act (Chapter 290) Section 3.
41 Penal Code (Chapter 224), Section 298.
43 Penal Code (Chapter 224), Sections 499-500.
ment as a way to protect citizens from cyberstalking, bullying and other troubling social trends. Under the law, a person who uses “threatening, abusive or insulting” expression likely to cause “harassment, alarm or distress” can be fined up to SGD5,000 (US$3,500). If done intentionally to cause harm, the offender can also be imprisoned for up to six months. If it includes a threat of violence, the jail term can be raised to 12 months. A separate provision in the Act protects public servants and public service workers from “indecent, threatening, abusive or insulting” expression when carrying out their work. An offender is liable for a fine of up to SGD 5,000 and up to 12 months in jail. Similar penalties are provided for stalking – which would cover, for example, repeated suggestive e-mails that would be reasonably known to cause harassment, alarm or distress. For all these provisions other than the one covering public officers, the victim can seek damages through civil proceedings. Victims can also apply to the court for a protection order, which could include prohibiting continued publication of the offending communication. The government also inserted into the law a section providing civil remedies for “false statements of fact” published about a person. The affected party can seek a court order requiring that the publication of the falsehood cease unless a notice is inserted setting the record straight. Although the Act was presented in parliament as a means of protecting ordinary citizens, it was quickly wielded by the government as a new instrument against critics (see Prosecutions and Detentions for Online Activities).

Prosecutions and Detentions for Online Activities

The new Protection from Harassment Act was marshaled by the Ministry of Defense in January 2015 in response to an online article written by an inventor with whom it was involved in a patent dispute. The Attorney General’s Chambers (AGC), acting for the ministry, invoked the law when it wrote to the writer and the website where the article appeared, The Online Citizen, to demand that they stop making and publishing “false statements.” Both the writer and the website challenged the government’s demand, arguing that the ministry does not qualify as a victim of harassment, being a large organization with the capacity to defend itself. The case had not been resolved by the end of the coverage period. The anti-harassment law was also used to stop a satirical Facebook page, SMRT Ltd (Feedback), from insulting Wendy Cheng, a blogger who has become a celebrity in her own right. Cheng’s popular Xiaxue blog has been criticized by more progressive bloggers for its intolerant and reactionary views. She successfully applied for a protection order, stopping the satirical group from making more insulting or abusive comments against Cheng and her family.

A teenaged blogger, Amos Yee, was also charged under the new anti-harassment law over online postings celebrating the death of founding prime minister Lee Kuan Yew. However, prosecutors requested an acquittal on the harassment charge after the court found Yee guilty on two other charges in May 2015. During the week of national mourning, the 16-year-old had posted a video of himself arguing why Lee did not deserve respect. At one point, the expletive-ridden commentary likened the delusions around Lee Kuan Yew to the beliefs of Christians. He was found guilty, under Section 298 of the penal code, of deliberately wounding religious feelings. Responding to a comment by the late British Prime Minister Margaret Thatcher that Lee was usually right, Yee had also posted a

---

49 SMRT Feedback/ The Vigilanteh, Facebook Community Page, http://on.fb.me/1moPOZm.
50 XiaXue (blog), http://xiaxue.blogspot.com/.
manipulated image depicting the two politicians having sex. For this, he was found guilty of obscenity under Section 292. In view of his age, the prosecution proposed probation. Public opinion was sharply divided over this highly publicized case, with many arguing that Yee, as a child, should have just been ignored.\footnote{Kirsten Han, “COMMENT: What Amos Yee is going through is far bigger than just one boy,” Yahoo!, April 20, 2015, \url{http://bit.ly/1R048st}.} Petitions and a public rally were organized in his support.\footnote{“Statement on the arrest of Amos Yee,” The Online Citizen, April 21, 2015, \url{http://bit.ly/1VFv4z9}; “Rally at Hong Lim Park calls for Amos Yee’s release,” Today, July 5, 2015, \url{http://bit.ly/110pbdk}.} However, the affair also revealed a strong reactionary streak within the Singapore public. Multiple complaints had been made to the police about Yee’s video. One man ran up to Yee outside the court and slapped him for insulting Lee Kuan Yew, for which he was sentenced to three weeks in jail.\footnote{Zaihan Mohamed Yusof, “Man jailed three weeks for slapping Amos Yee ‘lost control’,” AsiaOne, May 14, 2015, \url{http://bit.ly/1jdJ875}.}

In February 2015, two administrators behind the anonymously run political site, The Real Singapore (TRS), were arrested under the Sedition Act over a report on an annual religious procession. A scuffle had broken out involving devotees who were playing drums.\footnote{Lim Yi Han and Danson Cheong, “Cops arrest three for scuffle during Thaipusam festival,” AsiaOne, February 5, 2015, \url{http://news.asiaone.com/news/singapore/3-nabbed-over-scuffle-cops-during-thaipusam-procession#sthash.hMFwhNHv.dpuf}.} The Real Singapore published a report claiming that the complaint about noise had originated from a Filipino family.\footnote{“VIDEO: Local Singaporeans complain of Police Brutality at Thaipusam Procession,” February 4, 2015, accessed March 15, 2015, \url{http://bit.ly/1VFv4z9}.} The widely shared article, which was never substantiated, drew many negative comments against Filipinos.\footnote{Kimberly Spykerman, “The Real Singapore duo slapped with 7 charges under Sedition Act,” Channel News Asia, April 14, 2015, \url{http://bit.ly/1VEDETS}.} The TRS editors, Yang Kaiheng and Ai Takagi, were charged in April on seven counts of publishing seditious material on the TRS website and Facebook page. They faced a fine of up to SGD 5,000 (US$3,500) and three years’ jail on each charge. The charge sheet said that the offending articles had the “tendency to promote feelings of ill-will and hostility between different groups of people in Singapore”, namely, ethnic Indians and Philippine nationals.\footnote{Elena Chong, “Former Filipino nurse charged with sedition, giving false info to police,” The Straits Times, April 7, 2015, \url{http://bit.ly/1NocHQB}.} In May 2015, Yang was allowed to leave Singapore to visit his ailing father in Australia.

The Sedition Act was also leveled at a Filipino nurse working in a Singapore hospital, for Facebook comments that the authorities said could promote feelings of ill will and hostility between Singaporeans and Filipinos in the country.\footnote{“Filipinos disgusted by Ello Ed Mundsel Bello’s anti-Singaporean Comments,” The New Paper, January 10, 2015, \url{http://bit.ly/1Rul6Qs}.} Ello Ed Mundsel Bello allegedly said that he would be “praying that disators [sic] strike Singapore and more Singaporeans will die than I will celebrate;” and that he would “kick out all Singaporeans” and turn the country into a new “Filipino state.” As he initially denied posting the comments, he was also charged with providing false information to investigators. The sedition cases were indicative of the highly charged debates over immigration policy. Singapore has seen a trend of online xenophobia against Filipinos and other expatriates: in May 2014, the Filipino community canceled a planned Philippine Independence Day celebration at a shopping mall after encountering heated online opposition, including threats by Singaporeans to disrupt the event.\footnote{“Organisers cancel Philippine Independence Day event: Police,” Today, May 27, 2014, \url{http://bit.ly/1Om1JD7}.}
Singapore

tion by a government leader, and was seen by commentators as evidence of a souring of relations between the ruling party and critical segments of the public. Ngerng’s blog, *The Heart Truths*, had regularly accused the government of providing citizens with inadequate returns from the Central Provident Fund (CPF), a national pension scheme built on compulsory contributions from employees and employers. In one blog, he published a graphic illustrating the connections between the CPF Board, the government’s investment arms, and the prime minister, comparing this to a second graphic, from a news site, showing the organizational structure of a church whose leaders were in court charged with misappropriating funds. Lee’s lawyers said that the blog was thus claiming that the prime minister was guilty of criminal misappropriation of Singaporeans’ money. They rejected Ngerng’s initial apology and his offer of SGD 5,000 (US$3,500) in damages, pointing out that Ngerng emailed similar allegations to the media even after apologizing. In January 2015, the High Court ordered him to pay SGD 29,000 (US$20,700) in costs. As of May 2015, the damages in the civil suit had yet to be assessed. In early 2015, blogger Alex Au was convicted and fined SGD 8,000 (US$ 5,700) for scandalizing the judiciary. He is appealing the verdict. His offending 2013 blog had questioned the Supreme Court’s handling of a constitutional challenge to Section 377A of the penal code, which criminalizes sodomy.

Surveillance, Privacy, and Anonymity

While many people communicate anonymously online in Singapore, registration is required for some forms of digital interaction. Government-issued identity cards or passports must be produced when buying SIM cards, including prepaid cards, and buyers’ details must be electronically recorded by vendors. Registration for the Wireless@SG public Wi-Fi network also requires ID. Website registration requirements, although imposed on only a small number of platforms, have raised concerns about unwarranted official intrusion into their operations. In late 2013, the owner of one site declined to register because the MDA required the names of anyone involved in the “provision, management and/or operation of the website,” including volunteers.

Surveillance is “an accepted but hidden fact of life” and “few doubt that the state can get private

---

data whenever it wants.”71 Under the sweeping Computer Misuse and Cybersecurity Act, the minister for home affairs can authorize the collection of information from any computer, including in real time, when satisfied that it is necessary to address any threat to national security.72 Court permission need not be sought. Failure to comply with such orders is punishable with a fine of up to SGP 50,000 (US$35,000), a prison term of up to 10 years, or both. Under the Criminal Procedure Code, police officers investigating arrestable offenses may at any time access and search the data of any computer they suspect has been used in connection with the offense.73 No warrant or special authorization is needed. Penalties for non-compliance can include a fine of up to SGP 5,000 (US$3,500), six months in prison, or both. With authorization from the public prosecutor, police can also require individuals to hand over decryption codes, failing which they are liable to fines up to SGP 10,000 (US$7,000), jail terms up to three months, or both.

In 2013, international news reports said information leaked by former U.S. National Security Agency contractor Edward Snowden revealed SingTel had facilitated intelligence agencies’ access to the traffic carried on the major undersea telecommunications cable, SEA-ME-WE-3,74 but the news did not provoke an outcry among Singaporeans. Members of parliament and other commentators did appeal for more transparency regarding official surveillance efforts. Responding to a parliamentary question, the government said in October 2013 that, as part of the evidence gathering process, law enforcement agencies made around 600 information requests a year to Google, Facebook, and Microsoft between 2010 and 2012. Most were for Computer Misuse and Cybersecurity Act offenses, while the rest were for crimes such as corruption, terrorist threats, gambling, and vice. Although all requests were for metadata, agencies can request content data if required for investigating offenses, the government said.75 The Personal Data Protection Act enacted in 2012, which came into force in July 2014, exempts public agencies and organizations acting on their behalf.76

Singapore has adopted a U.S. Defense Department concept, “Total Information Awareness,” to gather electronic records en masse to look for digital footprints that might provide clues of impending security threats. The idea, which has proven controversial in the United States, has been incorporated into Singapore’s Risk Assessment and Horizon Scanning program. According to one analyst, “Singapore has become a laboratory not only for testing how mass surveillance and big-data analysis might prevent terrorism, but for determining whether technology can be used to engineer a more harmonious society.”77

Intimidation and Violence

There were no violent incidents targeting internet users in the past year, other than the assault on Amos Yee, for which the attacker was jailed (see Prosecutions and Detentions for Online Activities).

72 Computer Misuse and Cybersecurity Act (Chapter 50A) Section 15A.
73 Criminal Procedure Code (Chapter 68) Section 39.
77 Shane Harris, “The Social Laboratory,” Foreign Policy, July 29, 2014, http://atfp.co/1jOKyVI.
Singapore

However, there was one case of intimidation that led to the cancelling of an event. After Filipinos in Singapore publicized through Facebook their plans to organize a Philippine Independence Day celebration at a downtown mall, the news drew strong protests online. The prime minister came out in support of the planned event, which appeared only to increase the volume of xenophobic rhetoric and criticism of Singapore’s immigration policies. A week before the event, planned for June 2014, the organizers announced that they were calling it off, following advice from the police about public order and safety concerns at the venue. The authorities’ apparent surrender to online intimidation was surprising for a country that prides itself on law and order.

Technical Attacks

After several high-profile attacks on government and private-sector websites in recent years, as well as growing concern about cybercrime, more attention is being paid to cyber-security. A Cyber Security Agency was established in April 2015 to mitigate attacks and protect critical sectors such as energy, water, and banking.

---

78 “Organisers cancel Philippine Independence Day event: Police.”
79 Irene Tham, Shielding govt websites in cyber attacks,” AsiaOne, October 6, 2014, http://bit.ly/1WNWS6X.
South Africa

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>26</td>
<td>27</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Population:</td>
<td>53.7 million</td>
</tr>
<tr>
<td>Internet Penetration 2014:</td>
<td>49 percent</td>
</tr>
<tr>
<td>Social Media/ICT Apps Blocked:</td>
<td>No</td>
</tr>
<tr>
<td>Political/Social Content Blocked:</td>
<td>No</td>
</tr>
<tr>
<td>Bloggers/ICT Users Arrested:</td>
<td>No</td>
</tr>
<tr>
<td>Press Freedom 2015 Status:</td>
<td>Partly Free</td>
</tr>
</tbody>
</table>

Key Developments: June 2014 – May 2015

• An active signal jammer was discovered in parliament at the president’s annual State of the Nation address in February 2015, which blocked mobile networks and internet signals for at least an hour before the president’s speech (see Restrictions on Connectivity).

• Concerns over the independence of the telecommunications regulator, ICASA, arose in October 2014 when the minister of communications abruptly dismissed four of ICASA’s nine councilors (see Regulatory Bodies).

• A March 2015 Equality Court ruled that singer Sunette Bridges should be responsible for moderating and removing hate speech from her public Facebook page, setting a worrying precedent regarding liability for third party comments on websites and social networking platforms (see Content Removal).

• The Film and Publications Board introduced the Draft Online Regulation Policy in March 2015 that aims to protect children from harmful online content by allowing the government to pre-censor or take-down existing content that fails to meet the board’s new classification requirements (see Content Removal).

• Leaked documents known as the “Spy Cables” reported by Al Jazeera in March 2015 led to increasing concerns over the government’s surveillance intentions and capabilities (see Surveillance, Privacy, and Anonymity).
Introduction

South Africa’s digital media environment is generally free and open. A culture of free expression exists online, and the online sphere remains diverse and active. Access is a core concern for both civil society and the private sector, which has led to collaborative efforts between public and private players to expand access to information and communication technologies (ICTs). In 2014-2015, however, ICT development was constrained by the restructuring of the communications ministry into two departments and questions regarding the independence and effectiveness of the communications regulator, the Independent Communications Authority of South Africa (ICASA).

While the South African government under President Jacob Zuma has not proactively restricted access to ICTs or internet content, sporadic incidents in recent years caused concerns. During the president’s annual State of the Nation address to parliament in February 2015, an active signal jammer was discovered in parliament, which blocked mobile networks and internet signals for at least an hour before the president’s speech. Opposition parties and civil society members suspected deliberate government interference.

Certain types of online content came under judicial or regulatory scrutiny during the coverage period. In March 2015, an Equality Court ruling that Afrikaans folk singer Sunette Bridges should be responsible for moderating and removing hate speech from her public Facebook page led to concerns that the case sets a dangerous precedent regarding liability for third party comments on websites and social networking platforms. Also in March, the Film and Publications Board (FPB) proposed the Draft Online Regulation Policy that aims to protect children from racist, harmful and violent content online by allowing the FPB to pre-censor online content or take-down existing content when it fails to meet certain classification requirements. The FPB regulations, as well as the Equality Court ruling on moderating social media comments, could mean a new stringent regime of intermediary liability and enforcement for South Africa’s internet users.

Meanwhile, persistent concerns over government surveillance increased following reporting by Al Jazeera in February 2015 on leaked documents dubbed the “Spy Cables,” which detailed the foreign surveillance activities of South Africa’s State Security Agency. The government’s efforts to deal with the fallout from the leaked documents led to renewed pronouncements to pass the shelved Protection of State Information Bill, which had been vetoed by President Zuma in 2013 due to questions over its constitutionality. The bill contains provisions to criminalize whistleblowers and some journalistic activity, and to allow for the classification of a large degree of state information as state secrets.

Obstacles to Access

An active signal jammer was discovered in parliament at the president’s annual State of the Nation address in February 2015, which blocked mobile networks and internet signals for at least an hour before the president’s speech. Concerns over the independence of the telecoms regulator, ICASA, arose in October 2014 when the minister of communications abruptly dismissed four of ICASA’s nine councilors.

Availability and Ease of Access

Internet penetration has expanded rapidly in South Africa, though many believe that the expansion has not kept up with the country’s socioeconomic development. According to the latest data from
South Africa

the International Telecommunication Union (ITU), internet penetration reached 49 percent of the
South African population in 2014, up from 46 percent in 2013.¹ By contrast, mobile phone penetra-
tion reached 150 percent in 2014,² with the majority of internet users accessing the internet on their
mobile devices.³ Meanwhile, the country’s average internet connection speed is 3.2 Mbps (compared
to a global average of 4.5 Mbps), according to Akamai’s fourth quarter “State of the Internet” report
for 2014.⁴

In a 2014 national household survey, the country’s statistics agency reported that 10 percent of
South African households had access to the internet at home.⁵ Furthermore, according to the ITU,
only 3 percent of South African households possess fixed-line broadband subscriptions.⁶ Another
survey found that internet users were disproportionately white (50 percent), and speak either English
(65.5 percent) or Afrikaans (39 percent).⁷

A monopoly in the fixed-line market remains a challenge to reducing overall fixed-line broadband
costs, and there remains a general perception that mobile operators overcharge to maximize profits.
The passage of South Africa Connect—a new broadband policy that aims to connect 15 under-ser-
viced municipalities, and by 2030, the entire country—as well as a program providing tablets to
schools suggest a positive trend in increasing internet access, especially for the poor.⁸

South Africa is one of the few countries in the world that has failed to start the digital broadcasting
migration process, missing the deadline of June 17, 2015 set by the ITU. Consequently, South Afri-
cans will have to wait much longer to make use of higher quality wireless broadband services such
as LTE and WiMax that would be available on the spectrum freed up by the digital migration process.

Restrictions on Connectivity

The South African government does not have direct control over the country’s internet backbone
or its connection to the international internet. International internet connectivity is facilitated via
five undersea cables—SAT-3, SAFE, WACS, EASSy, and SEACOM—all of which are owned and oper-
ated by a consortium of private companies.⁹ Several operators oversee South Africa’s national fiber
networks, including partly state-owned Telkom and privately-owned MTN, Vodacom, Neotel, and
FibreCo, among others.¹⁰ Internet traffic between different networks is exchanged at internet ex-
change points (IXPs) located in Johannesburg, Cape Town, and Durban, which are operated by South
Africa’s nonprofit ISP Association (ISPA) and NapAfrica.¹¹

---

² As a result of separate subscriptions for voice and data services and the use multiple SIM cards in order to make use of
multiple product offerings, common among prepaid users. International Telecommunication Union, “Mobile-Cellular Telephone
³ As the Statistics South Africa survey also found, nearly 80 percent of households only have mobile phones. See: “South
Africa’s Internet access states revealed,” MyBroadband, August 26, 2013.
⁴ Akamai, “Average Connection Speed,” map visualization, State of the Internet, Q4 2014 Report, accessed May 29, 2015,
http://akamai.me/1LiS6KD.
⁶ International Telecommunication Union, “Fixed (Wired)-Broadband Subscriptions,” 2000-2014,
http://bit.ly/1UXKdD.
ly/1UXKdD.
¹⁰ “This is what South Africa’s Internet actually looks like.”
South Africa

While the diversity among South Africa’s gatekeepers to internet access ensures that the government cannot easily shut-down access to internet or mobile phone networks, the current government under President Zuma recently demonstrated its willingness to restrict access during certain events. In February 2015, an active signal jammer was discovered in parliament at the president’s annual State of the Nation address, which blocked mobile networks and internet signals for at least an hour before the president’s speech. The jammer would have continued to operate if opposition parliament members did not stage a protest upon discovery of the device. The presidency claimed it was a mistake in the protocol of the State Security Agency (SSA), which had forgotten to turn it off, while the Minister of State Security stated that the jammer was being used to prevent drones from flying above parliament. These explanations were rejected by opposition parties, technical experts, and many members of civil society, who suspected deliberate government interference. Following the incident, a group of media houses petitioned a high court to prevent the further use of jamming, however in May 2015, the Western Cape High court ruled that the state security agency had acted lawfully and was within its rights to use the jammer.

Meanwhile, scheduled power cuts as a result of load-shedding cause near daily interruptions of ICT access for most South Africans. Load-shedding is expected to last another two to three years, though carriers have made contingency plans in order to limit its effects on broadband services.

ICT Market

There are hundreds of ISPs in South Africa, with 174 ISPs belonging to the ISP Association (ISPA). However, the fixed-line connectivity market is still dominated by Telkom, a partly state-owned company of which the government has a 39.8 percent share and an additional 12 percent share through the state-owned Public Investment Corporation. Telkom effectively possesses a monopoly, despite the introduction of a second national operator, Neotel, in 2006. In the mobile market, there are five mobile phone companies—Vodacom, MTN, Cell-C, Virgin Mobile, and 8ta—all of which are privately owned except for 8ta, which falls under the partly state-owned Telkom.

Access providers and other internet-related groups are quite active in lobbying for better legislation and regulations. The ISPA is recognized as a self-regulatory body by the Department of Communications.

Regulatory Bodies

The autonomy of the regulatory body, the Independent Communications Authority of South Africa

---

14 Load-shedding is the scheduling of electrical outages over the distribution grid to avoid total blackouts due to under-capacity.
19 As reported in Freedom House 2013, Neotel has chosen to focus on providing wireless internet and telecom services, which has had minimal impact on last mile connectivity and the associated price of broadband.
South Africa

(ICASA), is protected by the South African constitution, although telecom observers contend that ICASA’s independence has weakened as a result of various incidents over the past few years.\(^{20}\) In May 2014, South Africa’s ICT ministry was split into two departments—the Department of Communications (DoC) and the Department of Telecommunications and Postal Services (DTPS)—resulting in ICASA being engulfed by the DoC rather than the DTPS, which created confusion and concern that the government was seeking more control over the regulator.\(^{21}\)

Concerns over ICASA’s independence deepened in October 2014 when the minister of communications abruptly dismissed four of ICASA’s nine councilors with immediate effect and without the mandatory requirement that councilors remain in office for a period of under 45 days until they have been replaced by a new councilor.\(^{22}\) As of mid-2015, no replacement councilors have been appointed, leading to speculation that the communications minister intends to reduce the overall number of councilors.\(^{23}\) Furthermore, ICASA lacks financial control given its dependence on the Financial Treasury for funding and perennially cites poor resources as one of its primary challenges.\(^{24}\)

The Film and Publications Board (FPB) also regulates media and internet content in South Africa, though it has departed dramatically from the censorship activities of its Apartheid-era predecessor. Today, the FPB focuses solely on content classification. Critics, however, have pointed to the FPB’s broadening powers following several amendments which increased the range of material classified by the Film and Publications Act (1996) and “reduced the independence of the Board and the transparency of its appointment process.” In addition, ISPs are required to register with the FPB and must reasonably prevent and report the distribution of child pornography through their services.

Limits on Content

A March 2015 Equality Court ruling that singer Sunette Bridges should be responsible for moderating and removing hate speech from her public Facebook page sets a worrying precedent regarding liability for third party comments on websites and social networking platforms. The Film and Publications Board introduced the Draft Online Regulation Policy in March 2015 that aims to protect children from harmful online content by classifying content and allowing the government to pre-censor or take-down existing content that fails to meet the classification requirements.

Blocking and Filtering

Neither the state nor other actors block or filter internet and other ICT content, and there is no blocking or filtering of content transmitted by mobile phones.

---


Content Removal

Non-technical measures such as legal, administrative, or other means have not been used to force the deletion of content from the internet. Access providers and content hosts are not legally responsible for third party content, nor are they required to censor content transmitted by their users.

Nevertheless, a March 2015 court ruling against a prominent figure in South Africa may set a precedent regarding intermediary liability for third-party comments made on social media and online news platforms. In late 2014, the South African Human Rights Commission took Afrikaans singer Sunette Bridges, known as a propagandist of (the discredited) “white genocide” in South Africa campaign, to the Equality Court on accusations that the singer was hosting hate speech comments on her public Facebook page, in violation of the Equality Act. In ruling that the comments from various fans indeed amounted to hate speech and harassment, the court ordered Sunette Bridges to regularly monitor her Facebook page and remove any content that could be considered hate speech, harassment, or incitement to violence.

The Electronic Communications and Transactions Act of 2002 (ECTA) requires ISPs to respond to takedown notices regarding illegal content such as child pornography, defamatory material, or copyright violations. Members of the ISPA—the industry representative body—are not held liable for third-party content that they do not create or select, though they can lose their protection from liability if they do not respond to takedown requests. As a result, ISPs often err on the side of caution by taking down content upon receipt of a notice to avoid litigation, and there is no incentive for providers to defend the rights of the original content creator if they believe the takedown notice was requested in bad faith. Meanwhile, any member of the public can submit a takedown notice, and there are no existing or proposed appeal mechanisms for content creators or providers.

In March 2015, the FPB proposed the Draft Online Regulation Policy, which will allow the FPB to pre-censor online content or take-down existing content that fails to meet certain classification requirements. Drafted for the purpose of protecting children from racist, harmful, and violent content online, the proposed policy will regulate commercial content published online, such as games and films, through a classification system managed by the FPB. Problematically, online content to be classified under the proposed policy also explicitly extends to any self-generated content, including Facebook posts, tweets, YouTube videos, or any other user-generated content created in the country. According to the policy, the FBP would have the power to “refer any self-generated video that is found to contain classifiable elements for classification to its classification committee, instruct the distributor to take down the unclassified content and only reinstate it after having complied with the FPB classification decision.” All new commercial content (for example, films and games) would be required to apply for classification by the FPB prior to publication, which if abused, could lead to the pre-publication censorship of political, social, or religious content. The regulations would also allow for the FPB to grant co-regulatory status to corporations, allowing them to classify their own content, and provides for a large budget for the training and deployment of “classifiers.” Public comments

---

25 South Africa has an equality court, for cases involving discrimination and hate speech. The Equality Court functions in the High Court system, and Equality Courts are High Courts.


South Africa

on the draft online regulations were due in mid-July. In August 2015, the South African Cabinet approved the introduction of the draft policy to parliament as the Film and Publications Amendment Bill.29

Media, Diversity, and Content Manipulation

Citizens are able to access a wide range of viewpoints and perspectives online. Web-only news platforms, such as the Daily Maverick, have attracted widespread attention in recent years. In some instances, key news stories have been broken online, illustrating how online media is growing as a primary source of news in the country. In line with this development, recent anecdotal evidence suggests that the South African youth are increasingly reliant on the internet and radio for information and are less dependent on television and print news for current affairs.30 Similarly, there are indications that in rural areas with internet access, the online versions of community newspapers are being accessed ahead of their print versions.31 Nevertheless, while both English- and Afrikaans-language content is well represented online, 9 of South Africa’s 11 official languages are underrepresented, including on government websites.

Online self-censorship is low in South Africa, and the government does not actively try to limit or manipulate online discussions. Nevertheless, ANC-aligned businessmen have made significant inroads into the media landscape by acquiring or launching new media products over the past few years, leading to concerns over increasing progovernment bias among prominent media outlets.

Digital Activism

The internet has become a successful tool for online mobilization and democratic debate in South Africa, and the use of the internet and other ICTs for social mobilization is uninhibited by government restrictions.

In the past year, citizens actively took to Twitter to cover, respond to, and criticize the State of the Nation address in February 2015, particularly the signal-jamming incident cut off journalists’ access to mobile and internet networks during the event (see “Restrictions on Connectivity”). South African netizens also actively used Twitter to share information and revelations about the Al Jazeera “Spy Cables,” which reported on leaked documents revealing the government’s foreign surveillance and intelligence gathering activities (see “Surveillance, Privacy, and Anonymity”).

Violations of User Rights

Persistent concerns over government surveillance increased following reporting by Al Jazeera in February 2015 on leaked documents dubbed the “Spy Cables,” which detailed the foreign surveillance activities of South Africa’s State Security Agency.

30 Suggested by Anton Harber, Professor of Journalism and Media Studies at the University of Witwatersrand.
31 Suggested in an access workshop held in East London in November 2013, run by Afesis-Corplan.
Legal Environment

The South African constitution provides for freedom of the press and other media, freedom of information, and freedom of expression, among other guarantees. It also includes constraints on "propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender, or religion and that constitutes incitement to cause harm." Libel is not a criminal offense, though civil laws can be applied to online content, and criminal law has been invoked on at least one occasion to prosecute against injurious material. The judiciary in South Africa is regarded as independent.

Prosecutions and Detentions for Online

Aside from the legal proceedings launched against singer Sunette Bridges for hosting hate speech comments on her public Facebook page (see Content Removal), individuals were not prosecuted, detained, or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs during the coverage period.

Surveillance, Privacy, and Anonymity

Persistent concerns over government surveillance increased following reporting by Al Jazeera in February 2015 on leaked documents dubbed the “Spy Cables,” which detailed the foreign surveillance activities of South Africa’s State Security Agency (SSA). While the leaked documents focused primarily on the SSA’s foreign affairs intelligence, one document revealed a secret agreement between the SSA and Zimbabwe’s Central Intelligence Agency to monitor and share information about “rogue NGOs” and “media, including social networks,” with an eye towards “subversive media.”

In response to the Spy Cables scandal, government officials including the minister of state security announced renewed intentions to pass the Protection of State Information Bill (POSIB), which had been vetoed by President Zuma in 2013 based on questions regarding its constitutionality. Provisions in POSIB—also known as the “Secrecy Bill”—pose a threat to freedom of expression, press freedom, and internet freedom. In an effort to regulate state information, POSIB would place harsh restrictions on the possession or distribution of classified state information with penalties of up to 25 years in prison. Individuals who intentionally access leaked information, including internet users, could be held criminally liable and face up to 10 years in prison.

Meanwhile, surveillance of domestic communications is regulated by the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA), which requires ISPs to retain customer data for an undetermined period of time. RICA also bans any communications system that cannot be monitored, placing the onus and financial responsibility on service providers to ensure their systems have the capacity and technical requirements for intercep-
South Africa

tion. While RICA requires a court order for the interception of domestic communications, the General Intelligence Laws Amendment Act (known locally as the “Spy Bill”) passed in July 2013 enables security agencies to monitor and intercept foreign signals (electronic communications stemming from abroad) without any judicial oversight.

RICA also compromises users’ right to anonymous communication, requiring mobile subscribers to provide national identification numbers, copies of national identification documents, and proof of a physical address to service providers. An identification number is legally required for any SIM card purchase, and registration requires proof of residence and an identity document. For the many South Africans who live in informal settlements, this can be an obstacle to mobile phone usage. Meanwhile, users are not explicitly prohibited from using encryption, and internet cafes are not required to register users or monitor customer communications.

Despite the legal framework for the interception of communications established under RICA, there have been worrying reports that the National Communications Centre (NCC)—the government body tasked with collecting intercepted signals—conducts surveillance without regard to RICA, thus extra-legally. In June 2013, an investigative report by the Mail & Guardian revealed that the NCC monitors mobile phone conversations, SMS, and emails, “largely unregulated and free of oversight.” According to the Mail & Guardian, the NCC also has the technical capacity and staffing to monitor both SMS and voice traffic originating from outside South Africa. Calls from foreign countries to recipients in South Africa can ostensibly be monitored for certain keywords; the NCC then intercepts and records flagged conversations. While some interceptions involve reasonable national security concerns, such as terrorism or assassination plots, the system also allows the NCC to record South African citizens’ conversations without a warrant and is subject to abuse without sufficient oversight mechanisms.

The Protection of Personal Information (POPI) Act, signed into law in November 2013, provides measures to protect users’ online security, privacy, and data. No law ensuring the constitutional right to privacy existed previous to POPI, which allows an individual to bring civil claims against those who contravene the act. Penalties for contravening the law are stiff, including prison terms and fines of up to ZAR 10 million (over US$900,000). However, the president has yet to set a commencement date for the new legislation as of mid-2015, after which point companies will have one year to begin compliance with the law.

Intimidation and Violence

There were no cases of intimidation or violence reported against online users or journalists during the coverage period.

---

Technical Attacks

South Africa is highly vulnerable to cybersecurity threats on many fronts, though independent news outlets and opposition voices were not subject to targeted technical attacks during the coverage period. Government websites are often hacked. Most of the hacks are perpetrated by amateur hackers with no apparent political motivations other than to advertise their skills, and consist of minor website defacements rather than incidents of data theft.

44 Through the use of a simple Google search trick, it is evident that a large number of websites have previously been “hacked” in some way or another. This can be emulated by googling the following: “hacked by” site:gov.za, or “hacked by” site:org.za. This will reveal the presence of the term “hacked by” in either governmental or NGO domains. The term is often used in the defacements. The search trick does not reveal up-to-date data, and many sites revealed have been fixed since their indexing.
South Korea

Key Developments: June 2014 – May 2015

- The Public Prosecutors’ Office set up a special investigation unit for enhanced monitoring of “online slanders and rumors” in September 2014, after the official response to an April 2014 ferry accident provoked widespread criticism (see Prosecutions and Detentions for Online Activities).

- Hundreds of thousands of smartphone messenger users switched from the most popular domestic provider to an encrypted, foreign alternative due to fears of surveillance (see Surveillance, Privacy, and Anonymity).

- In February 2015, the Seoul High Court jailed a former intelligence chief for three years for orchestrating an online smear campaign against the president’s rivals prior to the December 2012 election (see Media, Diversity, and Content Manipulation).

- Cyberattacks allegedly originating from North Korea targeted nuclear power plants in December 2014 (see Technical Attacks).

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>Partly Free</td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>33</td>
<td>34</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 50.4 million

Internet Penetration 2014: 84 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2015 Status: Partly Free
South Korea

Introduction

Advanced digital infrastructure in South Korea's vibrant democracy comes with a unique set of restrictions. Internet users face censorship rooted in political tensions with North Korea or traditional social values, and numerous laws restrict different aspects of digital activity. Observers point out that such restrictions have increased since the conservative party returned to power in 2008. Criminal investigations targeting online users are of particular concern. In 2013, the United Nations special rapporteur on the situation of human rights defenders called on South Korea to bring laws and practices affecting the right to freedom of expression in line with international standards.

During the coverage period, while Park Geun-hye of the conservative Saenuri Party was heading toward the halfway point in her five year presidential term, courts were still considering the case of online content manipulation by intelligence and military agents, which was allegedly conducting to aid Park's victory in the 2012 election. Furthermore, the sinking of Ferry Sewol in April 2014, resulting in hundreds of deaths, provoked widespread criticism of the Park administration's response to the disaster. In order to contain the criticism, public prosecutors sought heavy penalties for online defamation, which South Korean law punishes more severely than similar offenses offline.

Online privacy has been another prevailing issue for South Koreans. Despite a landmark ruling by the Constitutional Court in 2012 that stopped websites from registering users' national ID numbers and allowed for more anonymous interactions, cyberattacks and online theft have exposed millions of South Korean's personal details in the past five years. Courts have refused citizens permission to obtain new, uncompromised ID numbers. Moreover, domestic service providers legally provide the authorities with user data even without a warrant, introducing scope for abuse. In 2013, police accessed private social network accounts and real-time location information while investigating a railway union protest. In September 2014, a significant number of users left the country's most popular mobile messenger, Kakaotalk, which was alleged to be cooperating in a post-Sewol crackdown on criticisms of the government.

Obstacles to Access

South Korea boasts one of the world's highest broadband and smartphone penetration rates. The internet service sector is relatively diverse and open to competition, while the mobile market could be subject to more state influence. Broadcasting and telecommunications activities are regulated by

---

South Korea

Korea Communications Commission (KCC) and the content and ethical standards of such activities are monitored by the Korea Communications Standards Commission (KCSC). Both commissions are chaired by presidential appointees.

Availability and Ease of Access

South Korea is one of the most wired countries in the world, for both usage and connection speed. Internet penetration was at 84 percent in 2014. Counting access via mobile phone, television, and game consoles, an estimated 97 percent of households had access by 2012.

Several factors have contributed to the country’s high degree of connectivity. First, high-speed access is relatively affordable. Most residences have connections capable of reaching 100 Mbps for under KRW 30,000 (US$27) per month. Second, the population is densely concentrated in urban areas. Roughly 70 percent of South Koreans live in cities dominated by high-rise apartment buildings that can easily be connected to fiber-optic cables. Finally, the government has implemented a series of programs to expand internet access since the 1990s, including subsidies for low-income groups.

Mobile phone penetration was at 116 percent in 2014—a sign that many users now have more than one device. Moreover, the smartphone ownership rate rose to 84 percent as of December 2014, surpassing that of computers at 78 percent according to data released by the Ministry of Science, ICT and Future Planning (MSIP). Wi-Fi coverage has increased rapidly to accommodate smartphones and tablet computers. Free Wi-Fi is offered in over 2,000 public spaces across the country, including train stations, airports, libraries, health centers, and community centers. The MSIP has also announced its plan to further the coverage to 12,000 public hotspots by 2017.

Omnipresent and affordable cybercafes have helped prevent a digital divide in South Korea. Known as “PC bang” (“computer rooms”), many offer broadband access for approximately US$1 per hour, and also serve as venues for social interaction and online gaming. There is no significant gap in access to ICTs with respect to gender or income level, although differences persist across generational and professional lines.

6 Zoe Fox, “The 10 countries With the Fastest Internet,” Mashable, August 22, 2013, http://on.mash.to/1gs4CkK.
8 South Korea has been on the top of the Organisation for Economic Co-operation and Development’s (OECD) list of internet access rates in 34 member countries since 2000. OECD, “Households with access to the internet in selected OECD countries,” Key ICT Indicators, July 2012. http://bit.ly/19XqBzX.
11 Sutter, “Why internet connections are fastest in South Korea.”
South Korea

Restrictions on Connectivity

The country's internet backbone market is oligarchic, with Korea Telecom (KT) as the biggest provider. KT was founded in December 1981 and state-owned until privatization in 2002. The network infrastructure is connected to the international internet predominantly from the southern cities of Busan and Keoje, through international submarine cables, to Japan and China. For national security reasons, police and the National Intelligence Service have oversight on the access points, but the government is not known to implement restrictions on internet or mobile access for political reasons.\(^{17}\)

ICT Market

The telecommunications sector in South Korea is relatively diverse and open to competition, with 109 internet service providers (ISPs) operating as of March 2015.\(^{18}\) Nevertheless, it is dominated by three companies: Korea Telecom (42 percent), SK Telecom (25 percent), and LG Telecom (16 percent). The same firms also control the country’s mobile service market, with 27 percent, 46 percent, and 19 percent, respectively.\(^{19}\) All three companies are publicly traded, but they are part of the country’s chaebol—large, family-controlled conglomerates connected to the political elite, often by marriage ties.\(^{20}\) This has given rise to speculation that favoritism was at play in the privatization process and in the selection of bidders for mobile phone licenses.\(^{21}\) Korea Mobile Internet (KMI), a consortium of mobile virtual network operators who rent capacity from the main players, made a sixth attempt to enter the market in May 2014. In July, the MSIP rejected their bid for a license for failing to meet financial requirements, which a KMI spokesman described as “excessively strict.”\(^{22}\)

Under the stated aim of easing the information asymmetry caused by the effective oligopoly of the mobile phone market, an act came into effect in October 2014 limiting service carriers’ subsidies for consumers. However, it ended up hiking up the prices of mobile handsets and subscriptions, leading to a public furor, and is currently under reconsideration.\(^{23}\)

Regulatory Bodies

The conservative Lee Myung-bak government, which was in power from February 2008 to February 2013, restructured the regulatory institutions overseeing the ICT sector. The Ministry of Information and Communication and the Korean Broadcasting Commission merged to create the Korea Communications Commission (KCC) in February 2008, tasked with overseeing both telecommunications and broadcasting to improve policy coherence between the two sectors.\(^{24}\) The KCC consists of five commissioners, with the president appointing two (including the chairman) and the National As-

---

17 Interviews with ICT professionals, August 2015.
South Korea

The Assembly choosing the remainder. The KCC struggled to earn credibility, as its first chairman, Choi See-joong, was a close associate of President Lee, causing some observers to view the restructuring as a government effort to tighten control over the media and ICT sectors. Lee reappointed Choi as chairman in 2011, despite the objections of opposition lawmakers, who said that Choi’s personnel choices politicized the agency and that his licensing decisions favored conservative-leaning media outlets. Choi resigned in 2012, and was later sentenced to two and a half years in prison and a fine of KRW 600 million (US$545,000) for influence peddling. Lee pardoned him at the end of his term in January 2013.

In 2013, President Park Geun-hye missed an opportunity to distance herself from this history of cronyism, naming her close aide and four-term lawmaker Lee Kyeong-jae to head the KCC. She also transferred the KCC’s policy and strategy-related responsibilities to the new Ministry of Science, ICT and Future Planning. The KCC retains its regulatory remit and is currently led by a former judge, Choi Seong-joon.

The content of broadcasting and internet communications is qualitatively monitored by the Korea Communications Standards Commission (KCSC). Established in 2008, the KCSC is nominally an independent organization, but its nine members are appointed by the president and the National Assembly. The current chair of the commission is Park Hyo-jong, a key figure of the country’s neo-conservative movement.

**Limits on Content**

Although South Korean cyberspace is vibrant and creative, there are a number of restrictions on the free circulation of information and opinions. Technical filtering and administrative deletion of content is particularly evident. Content that “praises or benefits” communist North Korea or that undermines the traditional social values of the country is blocked or deleted based on the recommendations of the Korea Communications Standards Commission. Systematic manipulation of online discussions is also being investigated. Won Sei-hoon, the former chief of the National Intelligence Service, was sentenced to three years in jail in February 2015 for directing an online smear campaign against the rivals of the current president in the December 2012 election. The top court, however, granted Won a retrial in July 2015.

**Blocking and Filtering**

Censorship is predominantly carried out on the orders of the Korea Communications Standards Commission (KCSC). In 2008, its first year of operation, 4,731 websites or pages were blocked, and

---

27 “South Korean president issues controversial pardons,” BBC News, January 29, 2013, [http://bbc.in/L3ce7o](http://bbc.in/L3ce7o).
29 Six members are nominated by the president and the party with a parliamentary majority, while three are nominated by the opposition. Jeong-hwan Lee, “A private organization under the president? The KCSC’s structural irony” (in Korean), Media Today, September 14, 2011, [http://bit.ly/1aYoGOA](http://bit.ly/1aYoGOA).
30 Jung-a Song, “South Korea orders retrial of former spy chief Won Sei-hoon,” The Financial Times, July 16, 2015, [http://on.ft.com/1h5Ojr6](http://on.ft.com/1h5Ojr6).
South Korea

6,442 deleted;31 its activities have increased since then. A total of 97,095 websites or pages were blocked and 24,581 deleted in 2014.32

A team of 20 to 30 monitoring officers flag possible offenses, including obscenity, defamation, and threats to national security. Commissioners meet every two weeks to deliberate over flagged cases, and then issue censorship orders to content hosts or service providers.33 Noncompliant service providers face up to two years’ imprisonment, or a fine of up to KRW 10 million (US$9,000), under the Comprehensive Measures on Internet Information Protection issued by the KCC in 2008.34 Observers criticize the KCSC’s vaguely defined standards and wide discretionary power to determine what information should be censored, allowing the small number of commissioners to make politically, socially, and culturally biased judgments, often lacking legal grounds.35 Moreover, in many cases, the commission blocks entire sites even though only a small portion of posts are considered to be problematic. In March 2015, for example, the commission blocked the entire platform of an adult cartoon service, saying that part of its content was obscene. However, the service provider argued that the content was provided through an age-authentication system in compliance with the law. Faced with a public furor, the commission withdrew the shutdown order after only two days.36

Censored content is classified by categories including gambling, illegitimate food and medicine, obscenity, violating others’ rights, and violating other laws and regulations. The last category includes websites containing North Korean propaganda or promoting reunification, based on Article 7 of the 1948 National Security Act, which bans content that “praises, promotes, and glorifies North Korea.”37 The police and other authorities can refer matters to the commission, and individuals can also submit petitions. Police referred 1,281 items to the KCSC between January 2013 and August 2014 for jeopardizing national security.38

Content Removal

Police approached users and service providers directly and requested them to delete 22,928 items on national security grounds between January 2013 and August 2014, according to official figures.39

In 2011, the KCSC expanded their remit to social media, mobile applications, and podcasts, creating a team to systematically monitor platforms such as Twitter and Facebook for illegal content.40 Since

---

31 3,816 websites or pages were blocked for “encouraging gambling,” 549 for “disturbing social order,” and 366 for “obscenity”; 3,238 were deleted for “disturbing social order,” 1,460 for “obscenity,” 1,201 for “violating others’ rights,” 424 for “violence, cruelty, and hatred,” and 119 for “encouraging gambling.”
32 Among those blocked, 40,029 were for “encouraging gambling,” 37,817 for “prostitution and obscenity,” 14,113 for “illegitimate food and medicine,” 3,425 for “violating other laws and regulations,” and 1,711 for “violating others’ rights.” Among those deleted, 8,804 were for “violating other laws and regulations,” 7,290 were for “illegitimate food and medicine,” 6,193 for “prostitution and obscenity,” 1,920 for “encouraging gambling,” and 374 for “violating others’ rights.” Statistics published quarterly by the Korea Communications Standards Commission at http://bit.ly/1iDTDgX (in Korean).
33 Author’s interview with Park Kyung Sin, who served as a commissioner until his resignation in 2014, at the KCSC office, April 4, 2013.
39 Chang, “66 years on, the National Security Act evolves into one for cyberland”.
40 Matt Brian, “South Korea may begin censoring social networking, mobile apps from next week,” The Next Web, December
South Korea

selectively deleting posts from Twitter and Facebook is more difficult than from websites and blogs, the KCSC first warns users to voluntarily delete posts containing false or harmful information. If they refuse, the commission then asks ISPs to block other users from accessing the disputed accounts. Social media cases amount to roughly five percent of the total considered by the KCSC, according to a former commissioner.  

Until recently, a major cause for concern was that authors of blocked or deleted content were never notified of the KCSC’s decision, nor given an opportunity to defend their right to publish. Affected users are allowed to challenge the commission’s ruling in principle, but with no independent avenue for appeal available, only 0.07 percent have actually done so. In a welcome development, a legal amendment passed on December 29, 2014, to mandate notifying owners of censored content before and after deletion. The effect of the addition, Article 25(2) to the Act of the Establishment and Operation of the Korea Communications Commission, is yet to be seen.

Under Article 44(2) of the Information and Communications Network Act, citizens who discover content they believe has violated their privacy or harmed their reputation can ask the intermediary company hosting the content to restrict it from view. On receiving a request, the company must hide the content in question away for the following 30 days. The content is then permanently deleted if its owner does not revise it or appeal within those 30 days. The clause was under review during the coverage period.

Under Article 44(3) of the same act, intermediaries are encouraged to monitor and carry out proactive 30-day takedowns of irregular content, even without a complaint. Companies who can demonstrate proactive efforts to regulate content would be favorably considered by the courts, while those who do not are potentially liable for defamatory or malicious content posted by third parties.

A copyright law that restricts file sharing was passed in 2009. Often referred to as the “three strikes rule,” it allows the Minister of Culture, Sports and Tourism, acting through the Korea Copyright Commission, to shut down an entire forum for failure to comply with a third warning to take down pirated content. Internet companies and civil liberties advocates say the law threatens fair use and free expression. In 2013, a controversy arose when the commission and the KCSC blocked U.S.-based music-streaming site Grooveshark, among other overseas torrent sites. Online freedom ac-

42 Interview with Kyung Sin Park.
45 “Comment on the government’s proposed amendment to the temporary takedown clause: the process for content restoration is desirable, the obligation of takedown is a step backwards” (in Korean), Open Net Korea, December 8, 2014, http://opennet.or.kr/7884.
tivists and some users of the site submitted an administrative litigation against the order in February 2014.50

**Media, Diversity, and Content Manipulation**

In December 2012, opposition lawmakers accused a National Intelligence Service (NIS) agent of manipulating 40 different online accounts to discredit opponents of then-presidential candidate Park Geun-hye. Police initially cleared the agent,51 but in 2013, prosecutors indicted former NIS director Won Sei-hoon on charge of authorizing agents to post thousands of online comments and 1.2 million tweets characterizing members of the political opposition as sympathizers of North Korea.52 Park Geun-hye denies ordering or benefiting from digital manipulation.53 Won and his successor, Nam Jae-joon, admitted having refuted North Korean propaganda in online forums but deny political motives.54 In September 2014, Won was given a suspended sentence under a law that bars intelligence officials from political activity, but acquitted of trying to sway the election.55 In December 2013, the Defense Ministry’s cyber command unit, launched in 2010 to “combat psychological warfare in cyberspace,” announced that some officials had posted inappropriate political content online during the same period, but without the knowledge of the unit heads; like Won Sei-hoon, they denied the more serious charge of election meddling.56

As of March 2015, while President Park was heading toward the halfway point in her single five year presidential term, the case was still far from a conclusion. Former chief of Seoul police, Kim Yong-pan, was cleared by the Supreme Court in January 2015 of charges of obstructing an investigation into the scandal.57 Despite the lower court’s ruling, Won was sentenced in February 2015 to three years in jail for smearing political candidates,58 but the Supreme Court ordered a retrial in July 2015.59 A sitting judge who had denounced Won’s earlier acquittal on an intranet was suspended for two months in December 2014.60

---

54 Ho-jin Song et al., “Nam Jae-joon says online posting is the NIS’s legit work. Also insists the allegation of election interference is a political set-up” (in Korean), *Hankyoreh*, August 5, 2013, [http://bit.ly/1aDobNP](http://bit.ly/1aDobNP).
58 “South Korea spy chief sentenced to three years in prison;” *BBC News*, February 9, 2015, [http://bbc.in/1dibHgp](http://bbc.in/1dibHgp).
59 Ju-min Park, “South Korea court orders retrial of ex-spy chief in vote-meddling case;” *Reuters*, July 16, 2015, [http://reut.rs/1iPkkVw](http://reut.rs/1iPkkVw).
South Korea

Attempts to manipulate content were evident again in April 2014 following a ferry disaster that cast the government in a poor light. An investigation subsequently revealed the vessel was operating illegally after being decommissioned, and that over 300 passengers—mostly high school students—died during an incompetent rescue operation. A newspaper reported the KCC had circulated an internal directive instructing ministries, broadcasting companies, ISPs, and the police to steer online discussions away from the topic. Out of 507 online items assessed by the KCSC in the two days following the directive, 72 were deleted, 25 were blocked, and 10 were referred to the police, according to news reports. The Ministry of Oceans and Fisheries separately issued a similar directive.

In May 2014, conservative legislator Han Sun-kyo proposed amending the Information and Communications Network Act to criminalize rumormongering on social networking sites “in times of disaster,” punishable by up to five years in prison or up to KRW 50 million (US$45,500) in fines. The proposed clause evolved from 47(1) of the 1983 Telecommunications Business Act, which was ruled unconstitutional in 2009.

Commissioner Park Kyung Sin resigned from the KCSC in protest at the government’s handling of information related to the incident in May 2014, saying that journalists echoing official briefings led news outlets to incorrectly report that all passengers had been rescued. In an open letter published on his blog, he said that KCSC censorship discourages government criticism, limiting the public’s ability to ensure oversight and accountability.

Digital Activism

South Korea’s overall media environment is partly restricted. In 2012, journalists launched a series of strikes against government interference and censorship for the first time since the country’s transition to democratic rule in 1987. A variety of alternative and activist media outlets developed online, including Newstapa, a user-funded investigative journalism platform. Since its January 2012 launch, it has accumulated about 35,000 regular donors, and became a leading source of information on the electoral manipulation scandal in 2013. The platform’s YouTube channel had been viewed more than 10 million times by early 2014. However, the KCC called the work of Newstapa and a handful of other independent news websites “pseudo journalism” in 2013, warning their owners not to report on issues outside their remit.

South Koreans have embraced online technology for civic engagement and political mobilization. When the Mayor of Busan opposed the screening of a documentary on the Sewol ferry tragedy at the southeastern city’s international film festival, and threatened to defund the festival, support was

---

62 Min-ha Kim, “In times of disaster, rumor-mongering through SNS should be punishable up to 5 years of imprisonment, says Han Sun-kyo” (in Korean), Mediasus, May 2, 2014, http://bit.ly/1sZO1mj.
67 Yoo Eun Lee, “South Korean authorities discredit dissenting voices.”
South Korea mobilized online and the documentary became the most downloaded film on popular web portals in February 2015.68

Violations of User Rights

South Koreans faced increasing challenges safeguarding their privacy online. The Public Prosecutors’ Office enhanced monitoring of “online slanders and rumors” in September 2014, addressing the president’s concern over the fast-spreading criticism of her administration after the Sewol ferry accident. A Japanese journalist who questioned the whereabouts of President Park during the accident was indicted for defamation in October 2014 and barred from leaving South Korea. Apprehensive about the crackdown, numerous Korean users left domestic services and fled to foreign alternatives including Telegram, a messenger service developed in Germany which offers some encryption. Besides government surveillance, citizens were exposed to cybersecurity threats as hackers targeted major infrastructure and personal data.

Legal Environment

The South Korean constitution guarantees freedom of speech, the press, assembly, and association to all citizens, but it also enables restrictions, stating that “neither speech nor the press may violate the honor or rights of other persons nor undermine public morale or social ethics.” South Korea has an independent judiciary and a national human rights commission that have made decisions upholding freedom of expression. Nonetheless, the continued prosecution of individuals for online activities has generated a chilling effect and international criticism.69

Several laws restrict freedom of expression in traditional media as well as online. The 1948 National Security Act allows prison sentences of up to seven years for praising or expressing sympathy with the North Korean regime. In 2010, the Ministry of Unification issued a notice reminding citizens that the 1990 Act on Exchanges and Collaboration between South and North Korea applies to online communications as well as offline,70 and that any visit to websites or pages maintained by people of North Korea must be reported to the government in advance.71 Anyone failing to do so faces a fine of up to KRW 1 million (US$900).

Defamation, including written libel and spoken slander, is a criminal offense in South Korea, punishable by up to five years’ imprisonment or a fine of up to KRW 10 million (US$9,000), regardless of the truth of the contested statement. Insults charges, which unlike defamation offenses must be instigated directly by a complainant, are punishable by a maximum KRW 2 million (US$1,800) fine or a prison sentence of up to one year. Defamation committed via ICTs draws even heavier penalties—seven years in prison or fines of up to KRW 50 million (US$45,500)—under the 2005 Information and Communications Network Act, which cites the faster speed and wider audience of online communication as a basis for the harsher sentencing.72

69 La Rue, “Full text of press statement.”
71 Reports of such contact, online and offline, are to be made through an online system at http://www.tongtong.go.kr/.
Prosecutions and Detentions for Online Activities

Prosecutions against individuals expressing North Korean sympathies have increased under conservative rule. In the first year of the Park Geun-hye administration, national security arrests increased 19 percent and detentions 37.5 percent.\(^{73}\) Between 2012 and 2014, 104 people were convicted for violation of the National Security Act in cyberspace, although a legislator of the ruling conservative party argued in April 2015 that the number should have been even larger considering an increase in the number of offenses being committed online.\(^{74}\)

Numerous online defamation cases have involved President Park Geun-hye. The month Park took office in 2013, a court in Incheon fined a citizen KRW 800,000 (US$720) for making libelous statements against her in the comments section of a news website six times during 2012.\(^{75}\) Another citizen, Huh, in Uijeongbu in Gyeonggi province, was given a one-year suspended jail sentence in the same year for 114 defamatory posts against Park on the conservative daily Chosun Ilbo’s website, including one calling her a “dictator’s daughter.”\(^{76}\) In a separate 2013 case, Pastor Cho Woong was sentenced to 18 months in prison for online videos alleging that Park had made a secret deal with Kim Jong-il, the late ruler of North Korea.\(^{77}\)

The Sewol ferry disaster prompted a series of legal actions. On September 16, 2014, President Park told a cabinet meeting that “profanity towards the president had gone too far” and that “insulting the president is equal to insulting the nation.”\(^{78}\) Two days after this remark, the public prosecutors’ office set up a special investigation unit for an enhanced monitoring of “online slanders and rumors.” In March 2015, the Supreme Court sentenced a 31-year-old citizen, Kim, to one year in prison for posting a fake screenshot of a messenger conversation suggesting that the Sewol rescue operation had been deliberately held back, although he deleted it within 10 minutes.\(^{79}\) In May 2015, a man in his 50s named Wu, who had repeatedly posted a conspiracy theory about the ferry disaster online between August and November 2014, was sentenced to 18 months in prison for defaming the coast guard.\(^{80}\) Separately, Japanese journalist Tatsuya Kato of the Sankei Shimbun newspaper was indicted for criminally defaming President Park in an August article that cited allegations about the president’s response to the disaster, though the same content was first published in a domestic daily, Chosun Ilbo, and spread across online media. The journalist was barred from leaving South Korea for eight months until April 2015 and faces up to seven years in prison.\(^{81}\)

79. “A white-collar man who had distributed a fake KakaoTalk on Sewol found to be guilty of cyber defamation” (in Korean), Kyunghyang Shinmun, March 1, 2015, http://bit.ly/1F0f0s.
In a non-political context, a plastic surgery patient who posted 46 complaints of malpractice online between April and June 2014 was fined 3 million KRW (US$2,700) in May 2015 for “cyber defamation,” which free expression advocates say is not an appropriate charge.82

Surveillance, Privacy, and Anonymity

Within South Korea, anonymous communication typical of the internet was long compromised by the so-called “internet real-name system” first adopted in 2004 as part of an amendment to the Public Official Election Act.83 Users were required to verify their identities by submitting their Resident Registration Numbers (RRNs) to join and contribute to web portals and other major sites. An RRN is a 13-digit number uniquely assigned to a Korean citizen at birth. In 2007, the real-name system was expanded to apply to any website with more than 100,000 visitors per day under Article 44(5) of the Information and Communications Network Act.

In 2012, the Constitutional Court ruled Article 44(5) unconstitutional, citing privacy vulnerabilities from cyberattacks among other factors.84 In 2011, a cyberattack allegedly originating from China targeted the popular portal Nate and its social networking service Cyworld. Hackers reportedly stole the personal details of 35 million users, equivalent to 70 percent of the population, including names, passwords, RRNs, mobile phone numbers, and email addresses. The portal’s parent company, SK Communications, said RRNs and passwords were encrypted,85 but the incident renewed public concern about internet users’ right to privacy.86 Around 2,900 users together filed a damage suit, but the Seoul High Court ruled in favor of the company.87 Fifteen citizens also filed a lawsuit to be able to change their RRNs, but the Seoul Administrative Court and the Seoul High Court ruled against them. In mid-2015, the case was being heard in the Constitutional Court. In December 2014, it was reported that the Ministry of Government Administration and Home Affairs planned to consider citizens’ applications for new RRNs case-by-case in the near future.88

The Personal Information Protection Act was amended in 2013 to reflect the Constitutional Court’s 2012 ruling. Website administrators are now prohibited from collecting users’ RRNs, and must destroy those already on record. Effective from August 2014, failure to protect an individual’s RRN is punishable by fines of up to KRW 500 million (US$455,000).89 Mobile service providers still require users to provide their RRNs.

Other laws, such as the Public Official Election Act, the Children and Youth Protection Act, the Game Industry Promotion Act, and the Telecommunications Business Act, separately require internet users to verify their identities.90 To ensure compliance with these laws, the KCC is exploring identity ver-
South Korea

Identification methods alternative to the use of RRNs, such as Internet Personal Identification Numbers (i-PINs, overseen by the Ministry of Government Administration and Home Affairs), authenticated certificates (issued by banks and other organizations permitted to collect RRNs by Article 23 of the Network Act), and SMS verification. However, large-scale hacking attacks into the i-PIN system in February 2015, generating 750,000 counterfeit numbers, called for rethinking of the security framework at a more fundamental level.91

While court-issued warrants are required to access the content of private communications, service providers may “choose” to surrender individuals’ metadata without a warrant to investigative agencies,92 including police, prosecutors, and the National Intelligence Service, under Article 83(3) of the Telecommunications Business Act. However, at least one court ruling has encouraged companies to seek out more judicial oversight before complying with warrantless requests. In 2012, in a KRW 20 million (US$18,000) suit by a user against a major web portal service who provided personal information to police, the Seoul High Court overturned an earlier ruling and actually penalized the company for failing to demand a warrant to support the police request. The company was ordered to pay KRW 500,000 (US$460) in compensation.93

The ruling does not appear to have strengthened privacy safeguards. According to the latest official press release in May 2015, service providers fulfilled 508,511 such requests in the second half of 2014, a six percent increase over the number they executed during the same period in 2013.94 The number of requests to access the records or content of private communications has been decreased, from 132,070 to 127,153 and from 337 to 192 respectively.

User rights advocates say these numbers are misleading, since one request can affect many individuals over a long period of time.95 Service providers are also criticized for not fulfilling their legal duty of informing affected individuals. In most cases they refuse to respond when users inquire whether their data has been requested by the authorities.96 During a union protest against the government’s rail privatization plans in 2013, leading members of the Korean Railway Workers’ Union were sought by the police for “obstruction of business” under Section 314 of South Korea’s penal code. In the course of the search, police obtained individuals’ personal details from accounts linked to the union’s virtual community space on Band, a group chat platform operated by the domestic web giant Naver. The company confirmed police had accessed the platform, but “did not inform us about the range of the search, so the bigger problem is that we do not know how much of our personal information was exposed,” a union representative told the media.97

92 Metadata here includes the user’s name, RRN, postal address, telephone number, user ID, and dates of joining or leaving the service. To access the actual content of communications, a warrant is mandatory.
93 Kang, “Portal sites that neglected malicious comments liable for defamation.”
96 See also a public campaign by Open Net: “Reclaim the right to be informed when telecom companies disclose personal information” (in Korean), http://bit.ly/1GRAX6e.
South Korea

The April 2014 ferry disaster also prompted accusations of privacy violations and government surveillance. When 43 teachers wrote on the presidential office’s website that Park Geun-hye should step down for the poor handling of the disaster, the Ministry of Education ordered education offices around the country to identify and discipline those involved, prompting further protests.98

The most telling development was a closed-door meeting that public prosecutors held with major service providers in September 2014 to discuss how to curb rumormongering, including Kakaotalk, the country’s most popular mobile messaging application, according to news reports.99 The company dismissed public concern about its cooperation with law enforcement agencies, saying its compliance was prescribed by law.

Public trust in the company, however, was undermined in October 2014 during a press conference by Jung Jinwoo, a vice representative of the Labor Party charged with “causing public unrest” during a post-Sewol protest. Jung said prosecutors had accessed two months’ worth of his private Kakaotalk conversations, along with the personal details of his 3,000 contacts, as part of the investigation.100 Public prosecutors responded by asking the court to cancel Jung’s bail.101 Yong Hye-in, a university student who initiated a silence protest to show support and solidarity for Sewol victims and their families, also turned out to be another subject of Kakaotalk surveillance.102

In the wake of these revelations, some 400,000 users left the service for foreign alternatives perceived to be beyond the influence of the South Korean government, such as Telegram, a Germany-based messaging service which advertises encrypted connections.103 In order to regain user trust, Kakaotalk held an urgent press conference on October 13, 2014, where its CEO vowed to reject future data requests from the authorities, even those with warrants.104 The following month, it was reported that seven warrants were pending due to the company’s noncompliance.

Intimidation and Violence

There have been no reports of physical violence against online users.

Technical Attacks

A notable increase in technical disruptions in recent years has highlighted vulnerabilities in the country’s ICT infrastructure, a trend which continued during the coverage period. Reported violations of electronic data tripled between 2010 and 2013, from 54,832 incidents to 177,736, according to offi-

---

103 Sam Judah & Thom Poole, “#BBCtrending: Why South Koreans are fleeing the country’s biggest social network,” BBC News, October 10, 2014, http://bbc.in/1Mimz68
cial figures.\textsuperscript{105} Local and U.S.-based researchers alleged that North Korean authorities were behind the 2013 attacks on major banks, among other targets.\textsuperscript{106}

In December 2014, the country’s monopoly nuclear power company was subject to cyberattacks apparently aimed at stealing internal data, including plant blueprints and employees’ personal information.\textsuperscript{107} The energy ministry and the company jointly stated that the damage was non-critical. The hackers, who claimed they could disable the control system of the plants, were initially believed to be antinuclear environmental activists, but a special investigation team concluded in March 2015 that North Korea was once again the source. Three workers died of toxic gas inhalation at a construction site for a plant three days after the attacks, but there was no connection between the two incidents, a spokesperson said.\textsuperscript{108}

\begin{thebibliography}{10}
\end{thebibliography}
Sri Lanka

Key Developments: June 2014 – May 2015

- The defeat of Mahinda Rajapaksa in the 2015 presidential election and the progressive politics of his successor, Maithripala Sirisena, have strengthened internet freedom (see Introduction).

- Political websites that were formerly censored are now freely accessible, including ex-ile-run news website TamilNet, the first to be blocked by the previous regime (see Blocking and Filtering).

- Over the last year, there has been a considerable decline in rights violations, including violence, prosecutions and intimidation (see Violations of User Rights).

- Digital activism and public engagement with critical political and socioeconomic narratives has increased on social media as access increases each year (see Digital Activism).
Sri Lanka

Introduction

Internet freedom improved considerably in Sri Lanka following the defeat of Mahinda Rajapaksa in the January 2015 presidential election. After almost 10 years in power, the United People’s Freedom Alliance (UPFA) now finds itself on the opposition benches. Soon after swearing in as the 6th Executive President of Sri Lanka, Maithripala Sirisena formed an interim government with the United National Party (UNP) and appointed its leader, Ranil Wickremesinghe, as prime minister. A commitment to a fair and open society was clearly outlined at the inception of the interim government. Both President Maithripala Sirisena and Prime Minister Ranil Wickremesinghe promised to run a government that stays clear of blocking websites, intimidating journalists, and other draconian practices that characterized the previous government’s relationship with online and traditional media, including the curtailment of editorial freedom.

In line with these assurances, all websites earlier blocked by the previous government were accessible by May 2015, including the exile-run news website TamilNet, blocked since 2007 for reporting on civilian casualties of the military campaign against the Liberation Tigers of Tamil Eelam (LTTE), which ended in May 2009. Digital activism through online news websites, blogs and citizen media initiatives continues to strengthen as more people use the internet to access news, opinion and engage with diverse sources of information. In the lead up to the presidential election, Facebook and Twitter were used to launch voter education campaigns.

After months of political bargaining, the 19th Amendment to the Constitution was passed in parliament in April 2015. The amendment strengthened checks and balances on the executive presidency, restored term limits to the presidency, and empowered independent commissions. The Right to Information (RTI), which was included as an action point for President Sirisena’s first 100 days, was declared a fundamental right. However, RTI legislation – drafted, amended and approved by the cabinet following considerable public debate - was not presented and passed in parliament during the coverage period of this report. Moreover, concerns still exist about the transparency of the regulatory framework for ISPs and the independence of the Telecommunications Regulatory Commission (TRC). Legal and regulatory reform is still needed to consolidate the opening for internet and media freedom witnessed in the past year.

Obstacles to Access

Internet penetration in Sri Lanka continues to increase every year due to affordable internet rates provided by ISPs. Moreover, an increasing segment of the population has turned to smartphones in order to access the web. While low digital literacy continues to be an obstacle to widespread ICT use, it is encouraging to note that the number of people able to use a computer is increasing, with a rise from 20 percent in 2009 to 24 percent in 2012. The independence of Sri Lanka’s Telecommunications Regulatory Commission (TRC) continues to be in question, even under a new government, after President Sirisena appointed his permanent secretary as the head of the commission.

---

1 Maithripala Sirisena is the 6th Executive President of Sri Lanka and the 7th Overall President.
Availability and Ease of Access

Internet penetration was at 26 percent in 2014, up from 22 percent in 2013, as a continually expanding economic sector and growing youth population drove demand for online services. Mobile penetration rose from 96 to 103 percent in the same period. At the same time, according to the Central Bank of Sri Lanka, the country’s total internet connections grew by 68 percent due to an 86 percent increase in mobile internet connections in 2014. Internet connectivity is becoming more affordable, with the cheapest broadband connections priced at just under US$5 a month. In September 2014, Dialog offered free access to its Wi-Fi network for a period of one month. As of 2015, Dialog operates over 2,500 pay-to-use Wi-Fi hotspots around the country exclusively for its subscribers.

Free access to the internet was a major campaign promise of President Sirisena and was featured in his manifesto for the presidential election. A few months after his election, the interim government announced the availability of free Wi-Fi at 26 public locations around the country. The Information Communications and Technology Agency (ICTA) – the state agency responsible for implementing the plan – announced that free Wi-Fi would eventually be available at over 1,000 public locations.

While Wi-Fi coverage appears to be increasing every year, technology experts have voiced concerns about the reliability of speeds delivered through public Wi-Fi spots. ISPs are attempting to address the issue of speed with new and improved services. SLT introduced carrier-grade public Wi-Fi technology, allowing enterprises, institutions and other private sector entities to access island-wide hotspots with a username and password. While two IT parks are currently open in Jaffna and Mannar, in 2014 the Ministry of Information and Communication Technology announced that 10 more IT parks would be constructed around the country in order to boost the IT sector and public access to ICTs.

Increasingly affordable handsets and data packages have boosted mobile internet use, particularly among young people. In the third quarter of 2014, Sri Lanka’s mobile phone imports reached 1 million units, while the shipments of smartphones increased by 100 percent. The overall growth rate for the market has been consistent year on year, which has in turn contributed to an increase in the use of smartphones to access the internet. At present, it estimated that over 20 percent of the pop-

---

Low digital literacy represents a major barrier to ICT use. Although Sri Lanka’s literacy rate is approximately 91 percent, only 20 percent of the population was comfortable using computers in 2009. However, the 2012 census reported that this figure had increased to 24 percent. A higher percentage of young people (47.2 percent among the 10-15 age group) used computers in comparison to older age groups, according to the census. Digital literacy is lower in rural areas, where the high cost of personal computers limits access for lower-income families, schools with digital facilities lack corresponding literacy programs, and software is often incompatible with the Sinhala and Tamil languages. The ICTA has sought to address this imbalance as part of an e-Sri Lanka project by establishing rural community centers to promote ICT access and services. Some local journalists criticized aspects of the development, saying high-value contracts were awarded based on cronyism, while some facilities complained of faulty equipment.

Restrictions on Connectivity

Sri Lanka has access to multiple international cables, but the majority of the landing stations for these cables is controlled by Sri Lanka Telecom (SLT), the majority state-owned ISP. Lanka Bell, a private operator, controls only one landing station. SLT does not allow other telecommunications companies to connect to landing stations using their own fiber network and instead imposes price barriers by making competing players lease connectivity from SLT at significantly higher prices. The state’s control over the internet architecture in the country is problematic, especially when non-price barriers emerge, such as delays in responding to private companies’ requests for increased capacity.

There were no large-scale connectivity interruptions during the coverage period of this report, although they have occurred in the past. SLT temporarily severed internet and 8,000 mobile phone connections in the predominantly Tamil-speaking north and east in 2007, which was then the center of the conflict with the LTTE and is still a militarized zone. In April 2015, the military confirmed that it had released 1000 acres of land from high-security zones (HSZs) in the Northern province. However, militarization and the existence of other HSZs remains a serious concern.

---

14 “Sri Lanka’s mobile phone shipments reached 1mn units in 3Q: Smart phone shipments up 100 pct: Report”, LBO, December 25th, 2014.

---

730  www.freedomhouse.org
Sri Lanka

The war also caused severe lags in infrastructure development for the northern and eastern provinces. Since the war’s conclusion, the government has made up some of this ground, thereby boosting the regions’ economic growth. The process of development, however, has been criticized for causing issues with respect to land ownership that threaten to further marginalize the local Tamil community. 25 More positively, census data identified heavy internet usage in post-war minority districts in 2011 and 2012, citing Vavuniya in the Northern Province as the district with the country’s highest household internet usage. 26

ICT Market

SLT commands more than 50 percent of the market and has the largest fiber-optic national backbone. 27 While the broadband market is competitive, there is no legal requirement for SLT to sell backbone access to its competitors. The second largest player, Dialog Axiata, allows wholesale access to its fiber-optic rings, which are concentrated in populated cities. 28

With over 9 million subscribers, 29 Dialog Axiata is the largest mobile service provider, followed by Mobitel (over 5 million), 30 Etisalat (3.8 million), Airtel-Bharti Lanka (1.8 million) and Hutchison Telecommunications (1.4 million). 31 So far, only Dialog Axiata, Mobitel, Sri Lanka Telecom and Lanka Bell offer 4G LTE broadband services. 32 In November 2014, SLT, in partnership with Chinese telecom giant Huawei, launched the country’s first 100G network, which would provide 8 terabits per second transmission capability through a fiber-optic network. 33

Regulatory Bodies

As a national regulatory body, the TRC’s actions have consistently lacked transparency and independence. 34 Over the years, the TRC’s interventions to restrict online content and pronouncements on strengthening online regulation have been partisan, extralegal, and repressive. 35 Under a constitutional amendment forced through by the Rajapaksa regime and ratified in 2011—which also removed presidential term limits—the president was able to appoint the heads and members of all

---

27 Galpaya, Broadband in Sri Lanka: Glass Half Full or Half Empty.
28 Galpaya, Broadband in Sri Lanka: Glass Half Full or Half Empty.
31 The customer base figures for Etisalat, Airtel and Hutchison received from sources in each company (according to customer churn rates for June/July 2015).
34 Under the Telecommunications Act No. 21 of 1994, the Minister of Telecommunications and Information Technology has sole discretion in issuing licenses and imposition of license conditions based on the recommendations of the TRC.
commissions, subverting legislative guarantees for the independence of the TRC and other statutory institutions.36

In April 2015, President Sirisena and his interim government were able to undo this stranglehold on democratic processes by introducing and ratifying the 19th Amendment to the Constitution, which empowered independent commissions in the country and restored term limits to the presidency.37 The passage of the amendment in parliament was considered a significant step toward strengthening democracy in the country and overthrowing the authoritarian politics of the Rajapaksa regime.

During his presidency, Rajapaksa cemented control of the TRC by appointing his permanent secretary as its chairman. Following his election victory, President Sirisena followed his predecessor’s footsteps by appointing his permanent secretary, P. B. Abeykoon, as the head of the TRC.38 In addition, President Sirisena appointed M. M. Zuhair—a former member of parliament and diplomat—as the Director-General of the TRC. While no blocks on news websites have taken place so far during President Sirisena’s administration, the political appointments to the TRC do give cause for concern. In February 2015, after Rajapaksa’s defeat, a businessman lodged a complaint at the Financial Crimes Investigation Division (FCID) against the former chairman and former director-general of the TRC for the alleged misappropriation of TRC funds. At the end of the coverage period, evidence was being collected for further action.39

**Limits on Content**

*News websites that were previously blocked under President Rajapaksa’s rule are now accessible. The loosening of content restrictions on online media came about after the election of President Sirisena and his promise to end the authoritarian practices of his predecessor. Encouragingly, the unblocking of websites extended to TamilNet—the first website to be blocked by the previous government—which is now accessible across all ISPs. Digital activism remains vibrant in Sri Lanka, with a number of citizen media sites and new sites freely publishing content on political and socioeconomic issues in the country.*

**Blocking and Filtering**

Local and international freedom of expression groups have documented dozens of websites blocked at different times in Sri Lanka since 2007, though the interventions lack a legal framework or judicial oversight.40 Following his victory in the 2015 presidential election, President Sirisena moved quickly to dismantle the censorship regime imposed by his predecessor. Prime Minister Ranil Wickremesinghe assured journalists that they would be free to report on issues in the country without the fear of abduction and that authoritarian practices like internet censorship would not occur under the new government.41

---

41 Jason Burke and Amantha Perera, “Sri Lanka’s new president promises ‘no more abductions, no more censorship’,” *The
Despite consistent censorship under the previous government, blocks on websites were not properly coordinated or comprehensive, with some targeted websites available at times on one or more ISPs and at other times completely inaccessible. Officials cited ill-defined national security measures to legitimize this censorship, though websites were blacklisted for content related to human rights issues, government accountability, corruption, and political violence. During Mahinda Rajapaksa’s presidency, censors targeted opposition news sites and independent news, including Tamil websites, sites run by Sri Lankans in exile, and citizen journalism platforms, though usually without acknowledging a political or legal motive. As with the previous government, the current political order restricts access to pornography.42

Officials have the power to direct the TRC to blacklist content.43 Under the country’s telecommunications act, ISPs must apply to the Ministry of Mass Media and Information for a license according to specifications laid out by the TRC, who can make recommendations regarding whether or not a license is granted. The ministry can also impose conditions on a license, requiring the provider to address any matter considered “requisite or expedient to achieving” TRC objectives.44 It is not clear if the TRC can impose other financial or legal penalties on uncooperative telecommunications companies. To date, however, no company is known to have challenged TRC requests or sought judicial oversight.45

Examples of websites briefly blocked in the past under President Rajapaksa’s government include Tamil-language news websites and online content by Human Rights Watch and Transparency International.46 During the coverage period of this report, two more websites, the Sri Lanka Mirror and the Independent, were temporarily blocked, apparently for publishing news items that were critical of the previous government.47 The Colombo Telegraph website was blocked several times,48 including in March 2014,49 and remained inaccessible until the end of 2014.50 Following assurances given by President Sirisena about the unblocking of websites, all three became accessible across ISPs, as did the exile-run news website TamilNet, censored since 2007 for its support of the Tamil rebels.51

There is no independent body in Sri Lanka that content providers can turn to if they are censored. Instead, they must file a fundamental rights application with the Supreme Court to challenge blocking or other restrictions. Lack of trust in the country’s politicized judiciary and fear of retaliatory measures represent significant obstacles for the petitioner.52 In December 2011, one settled out of

---

44 Centre for Policy Alternatives, Freedom of Expression on the Internet, 30.
51 Local internet users reported it was patchily accessible through some fixed-line and mobile broadband networks during that time. See, Sanjana Hattotuwa, “TamilNet.com Accessible Once More in Sri Lanka via SLT ADSL.”
Sri Lanka

court, agreeing to several TRC conditions—such as removing links to blocked content—in return for restored access.53

The absence of clear laws and conflicting official statements also complicate the process of launching legal challenges. In 2011, officials acknowledged blocking at least five locally hosted news websites,54 including the Sri Lanka Mirror and Lanka-E-News, citing concerns about defamation in the wake of stories about corruption and human rights violations that implicated high-ranking officials. One official accused the sites of publishing “character assassinations” of the president, while another said they were blocked for failing to register with the media ministry.55 Members of the local Free Media Movement brought a fundamental rights petition challenging the Ministry’s grounds for blocking unregistered sites—which has no legal basis—but the Supreme Court rejected it in 2012.56

Content Removal

Documented cases of content removal are few and far between. According to Google’s Transparency Report, the previous government made two requests for the removal of content over a five-year period. Google complied with the most recent, submitted in December 2013, which it categorized as hate speech.57 There were no requests from the government for the restriction of content on Facebook during the coverage period of this report.

Media, Diversity, and Content Manipulation

Despite the history of restrictions, there are still diverse, accessible sources of information online in English, Sinhala, and Tamil, including on socioeconomic and political issues. YouTube, Facebook, Twitter and international blog-hosting services were accessible and widely-used for the anonymous or pseudonymous critique of governance, development, and human rights abuses during the coverage period of this report, though authorities have temporarily blocked website domains on blog platforms in the past.58

Citizen media site Groundviews and its sister site Vikalpa—which feature opinion, news, investigative journalism, photography, art and short videos generated by citizens—publish content that would otherwise not be covered by the mainstream media.59 In 2014, Groundviews announced the launch of Maatram, a new citizen journalism initiative that publishes reportage and other content aimed at Tamil readers across Sri Lanka and within the diaspora.60 Another website, the Republic Square, which started up in mid-2013, was a widely-read news platform that appeared to stop reporting after the

54  At least one of these sites – www.lankaenews.com - continues to be periodically blocked in the country.
presidential election in January. The Colombo Post—an online news platform run by journalists in Sri Lanka—started in late 2014 and has gradually become a popular source of news about politics and socioeconomic issues in the country. The platform appeared to have temporarily shut down operations in February 2015, but resumed reporting in mid-March.

In 2012, the media ministry under the previous government directed the cabinet to approve an amendment to the notorious Press Council Act No.5 of 1973, making news websites subject to the same draconian content regulation as traditional media. However, the amendment failed to define what constitutes “news,” providing leeway for authorities to scrutinize a wider range of online platforms like blogs or social media. The act prohibits the publication of profanity, obscenity, “false” information about the government or fiscal policy, and official secrets. It also allows the president-appointed council to impose punitive measures on the violators of its provisions, including possible prosecution. The legislation was dormant under previous administrations until President Rajapaksa reactivated it after the end of the war. Strenuous objections from the international freedom of expression community failed to prevent the government from extending the restrictions to digital media.

A week after this announcement, the media ministry also proposed an amendment to institute a hefty registration fee of LKR 100,000 (US$790), plus an annual renewal fee of LKR 50,000 (US$395), costs which threatened to inhibit the emergence of new websites and force existing ones out of operation. According to the final cabinet decision, the registration fee was approved at LKR 25,000 (US$190) and the annual renewal fee at LKR 10,000 (US$75). In spite of media freedom guarantees, the current government has not rescinded the registration directive imposed by its predecessors. The media ministry still overlooks the registration of news websites, although it does not appear to be strictly enforced.

In May 2014, former President Mahinda Rajapaksa reaffirmed his intent to regulate social media and stated that the government would take the necessary steps to prevent the internet from being used to cause “social and political unrest.” Under President Sirisena and the new interim government, no attempts had been made to regulate social media as of May 2015.

During Rajapaksa's presidency, officials actively encouraged self-censorship “on matters that would damage the integrity of the island,” and many mainstream news websites complied, increasing the importance of citizen journalism and exile-run sites in the media landscape. Online platforms of the main state-run newspaper and broadcasting network supported former President Rajapaksa when he was in power and the UPFA government. These and official government websites have waged smear campaigns against UPFA critics in the past. Under President Sirisena, however, tra-
Sri Lanka

ditional and new media outlets have become vocal critics of both sides of the political divide, freely expressing opinions and publishing reports that would have never been tolerated under Rajapaksa’s administration. In reaction to reports published about the government and the economy, Minister of Finance Ravi Karunanayake requested that media institutions and journalists avoid abusing the “media freedom that prevails under the new government”. Overall, the practice of self-censorship by journalists and media institutions appears to be diminishing in response to the interim government’s commitment to media freedom.

In early 2013, hate speech against the Muslim community spread online when a Sinhala Buddhist extremist group gained a considerable following on social media. The group’s violent rhetoric led to attacks on mosques and Muslim-owned businesses, as well as isolated incidents of assault. No legal action was taken against the group’s members, and prominent public officials—including the president’s brother, Defense Secretary Gotabhaya Rajapaksa—openly supported them. Some of the relevant social media pages have since been removed, and the intensity of online hate speech declined during the coverage period of this report, though without stopping altogether. There are still many pages on Facebook that continue to publish offensive material targeting Muslims and other groups.

Digital Activism

The internet has provided a great deal of scope for robust digital activism and engagement on political issues in Sri Lanka. In the lead up to the presidential election, the hashtag #IVotedSL was launched on Facebook and Twitter – a campaign that called on people to exercise their franchise on election day. Twitter and Facebook profile photos as well as digital posters were developed and shared by thousands of users, publicizing the campaign and encouraging other users to take the pledge. Following the conclusion of the presidential election, another independent campaign was initiated by citizens on Facebook and Twitter—#icanChangeSL and #wecanChangeSL—to carry forward the interest of the #IVotedSL campaign and to sustain a meaningful dialogue about shaping a new country.

Violations of User Rights

Apart from one journalist who was questioned by the CID about his reports on anti-Muslim violence and his association with Al Jazeera, there were no significant reports of intimidation, prosecution or assault. Physical attacks and threats against journalists, including many linked to government actors,
gradually decreased in the aftermath of the civil war. While the failure to investigate past incidents cast a long shadow during President Rajapaksa’s rule, the new government under President Sirisena has promised to initiate investigations into the murder and disappearance of journalists.

Legal Environment

While the right to freedom of speech, expression, and publishing is guaranteed under Article 14 (1) (a) of Sri Lanka’s constitution, it is subject to numerous restrictions for the protection of national security, public order, racial and religious harmony, and morality. There is no constitutional provision recognizing internet access as a fundamental right or guaranteeing freedom of expression online. A culture of impunity, circumvention of the judicial process through arbitrary action, and a lack of adequate protection for individuals and their privacy, compound the poor enforcement of freedom of expression guarantees.

The Supreme Court has called freedom of expression from “diverse and antagonistic sources” indispensable to democracy. In 2012, however, it rejected a fundamental rights petition brought by members of the local Free Media Movement questioning the media ministry’s right to block websites for failure to register. By doing so, it missed a critical opportunity to check the government’s use of vague directives to control online content. After a complaint was made to the Human Rights Commission of Sri Lanka about the blocking of two websites in May 2014, the commission said it would investigate, but that freedom of expression was subject to constitutional limits.

Several laws with overly broad scope lack detailed definitions and can be abused to prosecute or restrict legitimate forms of online expression. Computer crimes and intellectual property laws allow information contained within computers to be admissible in civil and criminal proceedings. Publishing official secrets, information about parliament that may undermine its work, or “malicious” content that incites violence or disharmony could result in criminal charges. In 2011, the Ministry of Justice mooted a new obscene publications act to extend anti-pornography laws to electronic media, but did not correct the existing act’s failure to define “obscene.” As of mid-2015, the Ministry has made no announcements regarding the legislation’s implementation and it is unlikely that it will be carried forward given the change in government.

In April 2015, President Sirisena proposed new legislation to ban hate speech and material that could “exacerbate religious and ethnic tensions.” This is interpreted as a move to counter growing religious extremism in the country, which has led to sporadic incidents of communal violence over the last two years. The legislation, to be included in the penal code, carries penalties of a two-year jail sentence and a fine. There are considerable concerns about the proposed law. A critical point is that it is not clear how hate speech is defined. Moreover, the overbroad provisions of the legislation could be harmful to free speech.

---

manipulated to restrict legitimate forms of expression. As of May 2015 the legislation had yet to be drafted and presented to parliament. However, media activists and journalists believe a law will be drafted after the parliamentary election in August 2015.

Under the former president’s government, there was continuous obstruction to right to information (RTI) legislation, which would promote citizens’ access to documents held by government agencies and ministries. The Lessons Learnt and Reconciliation Commission—a post-war commission of inquiry appointed by former President Rajapaksa in May 2010—recommended RTI legislation as a necessary step towards addressing past and ongoing rights violations. However, UPFA parliamentarians rejected an opposition-backed bill in 2011. As part of President Sirisena’s 100-day program, the new government promised to introduce RTI legislation in order to entrench good governance and transparency within the public sector. While the passage of the 19th Amendment to the Constitution recognizes RTI as a fundamental right, the parliament had yet to pass the legislation for it during the coverage period, which has been drafted and approved by the cabinet. Civil society activists have flagged serious concerns about certain provisions of the act, specifically with regard to national security, protection for whistleblowers, and the lack of a clear provision with regard to what type of information, when revealed by authorities, could not be disseminated or published for public consideration.

Prosecutions and Detentions for Online Activities

No detentions were reported during the coverage period of this report, though in July 2014, the Criminal Investigations Department (CID) questioned Dinouk Colombage, a journalist who works online, for several hours about his coverage of anti-Muslim riots in the southern town of Aluthgama and his association with Al Jazeera. He was released without charge.

While the previous government was in power, internet users faced criminal charges in relation to their online activities. In one egregious 2012 example, CID officials raided the offices of the Sri Lanka Mirror and Sri Lanka X News on grounds of “propagating false and unethical news on Sri Lanka.” The journalists were released on bail the day after their arrest, though investigators later said their computers contained further grounds for prosecution, including content that violated the Obscene Publications Act—although the alleged obscenity was unpublished—failure to register the website, ridiculing the president, and evidence of an attempted coup. While the case was finally set aside

due to the CID failing to conclude investigations, the journalists filed a fundamental rights petition with the Supreme Court citing illegal arrest and violations of their right to free expression.91

**Surveillance, Privacy, and Anonymity**

Extrajudicial surveillance of personal communications is prohibited under the Telecommunications Act No.27 of 1996. However, a telecommunications officer can intercept communications under the direction of a minister, a court, or in connection with the investigation of a criminal offence. There is no provision under the legislation that requires officials to notify users who are targets of surveillance, and many journalists and civil society activists believe their phone and internet communications are monitored. In late 2013, Dialog CEO Dr. Hans Wijesuriya denied the existence of a comprehensive surveillance apparatus in Sri Lanka but agreed that telecommunications companies “have to be compliant with requests from the government.”92

Sri Lanka lacks substantive laws for the protection of individual privacy and data. Official statements lauding state surveillance make this absence a particular concern for internet users,93 as do policies like website registration, which civil society groups fear could be used to hold registered site owners responsible for content posted by users, or to prevent government critics from writing anonymously.94 Digital activists in Sri Lanka also believe Chinese telecoms ZTE and Huawei, who collaborated with Rajapaksa’s government in the development and maintenance of Sri Lanka’s ICT infrastructure, may have inserted backdoor espionage and surveillance capabilities.95 In spite of the new government’s commitment to freedom of expression, transparency, and right to information, privacy advocates are still cautious about how existing surveillance technology could be utilized and intensified in the future. This is particularly relevant given that security surveillance in the north and east still continues.96

A Ministry of Defense program to register mobile phone users for the purpose of “curbing negative incidents” was introduced in 2008 and revisited in 2010 after service providers failed to ensure that subscribers registered.97 Real-name subscriptions are already normal procedure, but the call for registration in 2010 required further information, including photo identification and up-to-date residence...

92 ‘Dialog CEO Hans Wijesuriya: “No surveillance program in Sri Lanka, but telecoms have to comply”.’
Sri Lanka

tial details. Unregistered users risked disconnection if they failed to comply, though no cases were reported at the time.

Intimidation and Violence

There were no attacks on online journalists or internet users during the coverage period of this report.

Online reporters, like their counterparts in traditional media, were attacked by forces on both sides during Sri Lanka’s civil conflict. Unsolved cases include the 2005 murder of TamilNet co-founder Dharmeratnam Sivaram, who was found dead in a high-security area outside parliament.98 The UN Human Rights Council adopted a resolution urging the government to investigate war crimes in 2012, but the trend of violence against traditional journalists continued amid a culture of impunity.

International news reports and rights groups say soldiers acting on the orders of high ranking officials in the previous government were responsible for the notorious “white van” abductions of critics and activists—named after the vehicle often used to carry them out—a claim the previous administration denies.100 Lanka-E-News journalist and cartoonist Prageeth Ekneligoda has been missing since January 24, 2010, after the website backed the political opposition in elections.101 Officials say he sought asylum overseas.102 The inaction on his case, combined with other methods of intimidation including arson attacks and legal harassment, forced Lanka-E-News and its editor out of the country.103

In May 2015, President Sirisena restated that he intended to re-open investigations into all past murders and disappearances of journalists, including the case of Prageeth Eknaligoda.104

Technical Attacks

Cybercrime is a growing problem in Sri Lanka, with illegal breaches of social media and email accounts becoming more common.105 Cyberattacks have also targeted critics of Rajapaksa’s regime in the past, though no incidents were reported during the coverage period.

During anti-Muslim riots in Aluthgama, hackers disabled websites and released over 340 govern-

---

Sri Lanka

The previous government recognized the need to strengthen its defensive capability, yet critics fear technology bought for this purpose could be used to restrict legitimate expression. Following the implementation of the Computer Crimes Act in 2007, the government at the time established the Computer Emergency Readiness Team and Coordination Center (CERT|CC) in order to protect Sri Lanka’s digital data. In July 2014, CERT|CC developed a security arm to protect the digital infrastructure of banks in the country. There have been no pronouncements about further securitization of the web under the new government.

107 Centre for Policy Alternatives, Freedom of Expression on the Internet, 42.
Sudan

Key Developments: June 2014 – May 2015

- Access to the internet became more challenging for Sudanese citizens as internet prices surged while speeds declined dramatically (see Availability and Ease of Access).

- Extremely slow internet speeds were experienced in parts of the country during several politically contentious periods, leading to strong suspicions of government throttling (see Restrictions on Connectivity).

- A new Freedom of Access to Information Law passed in January 2015 classifies 12 types of information that are restricted from citizens. Observers believe the government passed the new law to legalize the withholding of information and its censorship powers (see Legal Environment).

- In the lead up to the April 2015 general elections, several online journalists and activists were arrested while numerous online news outlets were hacked (see Prosecutions and Detentions and Technical Attacks).
Introduction

Internet freedom in Sudan remained under threat in 2014 and 2015, as authoritarian President Omar al-Bashir’s government intensified its crackdown on critical voices in the lead-up to general elections held in April 2015. In an attempt to expand control over the political space, the government enacted numerous laws designed to increase its powers while minimizing opportunities for opposition. In January 2015, for example, the Sudanese parliament approved constitutional amendments that gave the president powers to appoint and remove senior officials, and established a new body of security forces under the control of the National Intelligence and Security Service (NISS), which was previously limited to intelligence gathering.

A new Freedom of Access to Information Law passed in January 2015 with the purported aim of increasing transparency has instead led to greater limitations, with provisions that detail 12 types of information that are restricted from citizens, such as national security and foreign policy information. The limits effectively leave no room for journalists or the public to access any information of consequence. Observers believe the government passed the new law to legalize the withholding of information and its censorship powers.

Meanwhile, government authorities made other concerted efforts to restrict critical information and silence the opposition, including proactively manipulating the online information landscape and arresting several journalists and activists for their online activities. Several hacking attacks against critical news websites and activists’ social media webpages were reported, escalating around the April 2015 general elections. While no critical news or opposition websites were blocked during the coverage period, Sudanese officials regularly demanded the blocking of online news outlets, particularly after the outlets criticized government officials or published articles about corruption.

Obstacles to Access

Access to the internet became more challenging for Sudanese citizens in 2014-2015 as a result of increasing costs and declining quality of services. Extremely slow internet speeds were experienced during several political contentious periods, leading to strong suspicions of government throttling.

Availability and Ease of Access

Access to information and communications technologies (ICTs) in Sudan slightly increased over the past year, with internet penetration reaching 25 percent in 2014, compared to 23 percent in 2013, according to the International Telecommunication Union (ITU). The number of users may be higher as internet-enabled mobile phones have become widespread and cheaper in recent years.

Despite the spread of ICT services, access to the internet became more challenging for Sudanese citizens in 2014-2015 as the cost of access surged amid declining quality and speeds. Telecom com-

---

2 “Sudanese constitution to be amended to grant more powers to security services: official,” Sudan Tribune, April 30, 2015, http://bit.ly/1GBjQvB.
4 “Deterioration of telecommunication services in Sudan and companies complain of piracy,” [in Arabic] Sudan Tribune, April
Sudan

Companies introduced new bundles at higher rates that did not deliver speeds as advertised, while old bundles experienced worsening speeds. According to Akamai’s 2014 “State of the Internet” fourth quarter report, 6 Sudan’s average connection speed declined by 73 percent during the September-December 2014 quarter alone, decreasing from 3.6 Mbps to 1.0 Mbps (significantly lower than the global average speed of 4.5 Mbps). Increasing tensions and violent clashes between government forces and rebel factions in Sudan’s conflict regions have also led to frequent service disruptions.

As of mid-2015, monthly mobile internet subscriptions cost between SDG 2.62 to 68 (US$0.62 to $11), up from SDG 2 to 9 in 2014—an increase of 31 percent for 100MB of data and around 600 percent for 1GB packages. As a result, mobile phone penetration in Sudan decreased slightly from 73 percent in 2013 to 72 percent in 2014. 7 USB internet modems for personal desktops or laptops cost between SDG 124 and 261 (US$22 to $46) per month, and monthly fixed-line broadband subscriptions range from SDG 26 to 200 (US$5 to $35), depending on the package.

Internet access at cybercafes, which are concentrated in market areas and popular around universities and dorms, has also become more expensive, with minimum charges ranging between SDG 3-15 (US $0.50-2.51) per hour, up from SDG 2-5 (US $0.35-0.87) in 2014—a 50 and 200 percent increase, respectively—though the number of cybercafes in Khartoum state has decreased noticeably since the early 2000s as mobile internet has become cheaper and more accessible to the public. As a result of increasing prices, mobile phone and internet access is still out of reach for the majority of the population in Sudan.

Furthermore, approximately 1.2 million citizens living in rebel-controlled areas in South Kordofan have extremely limited access to the internet. 8 Nearly two million internally displaced persons (IDPs) living in camps have no access whatsoever.

In a positive step, previous obstacles to access imposed by U.S. economic sanctions in place against the al-Bashir regime since 1997 were mitigated in February 2015, when the U.S. Treasury Department announced it was easing the long-standing sanctions. 9 The sanctions banned the import of ICT hardware and original software made by American companies, such as anti-virus, anti-malware, anti-tracking, and anti-censorship software and more secure ICT applications. The ban had been particularly punitive on Sudanese activists and ordinary citizens, whose use of outdated technologies and software made them vulnerable to malware and other technical attacks. Under the February amendments to the sanctions, these vital technologies can now be imported into the country. 10

Restrictions on Connectivity

Sudan connects to the global internet through three international gateways—the partly state-owned

---

10 U.S. Department of Treasury, “Publication of Sudan General License- Related to Personal communications,” February 17, 2015, http://1.usa.gov/1GeXnmr
Sudan

Sudan Telecom Company (Sudatel), Zain, and Canar Telecom—–which are connected via four submarine cables: Saudi Arabia-Sudan-2 (SAS-2), Saudi Arabia-Sudan-1 (SAS-1), Eastern Africa Submarine System (EASSy), and FALCON. Partial control over the international gateway has enabled the government to restrict internet connectivity during particular events in the past, such as during the September 2013 nationwide protests when the government shut down service of all telecom providers for nearly 24 hours.

In August 2014, a five-day internet blackout was reported in the West Darfur region of Sudan, negatively impacting hundreds of students who were unable to apply for university, though the cause of the disruption remains unclear. In many other parts of the country, extremely slow internet speeds were experienced during several political contentious periods in 2014-2015, leading to strong suspicions of government throttling. For example, in the lead-up to the one-year anniversary of the September 2013 protests, broadband connection speeds in Khartoum declined significantly from an average speed of 3.2 Mbps to 2.22 Mbps in September 2014, which observers believed was an intentional effort by the Sudanese government to impede anniversary protests. In October 2014, during a largescale campaign initiated online to raise awareness about the mass rape of 200 women in the Darfuri town of Tabit (see “Media, Diversity, and Content Manipulation”), internet connections were reportedly as low as 1.48 Mbps. During the April 2015 elections, speeds were also slower than average at 2.34 Mbps.

ICT Market

There is fairly strong market competition in Sudan’s telecoms sector among four licensed telecommunications operators: Zain, MTN, Sudatel, and Canar. All four providers are privately owned by foreign companies, with the exception of Sudatel, which has 22 percent of its shares owned by the government; the remaining shares are held by a foreign entity. The Sudanese government manipulates the telecommunications sector indirectly through Sudatel’s board of directors, which includes the current Minister of Finance and National Economy as the board’s chairman and the current Governor of the Central Bank of Sudan as a board member.

MTN and Sudatel both offer broadband internet, while Zain offers fast internet through its USB modem and mobile internet services. Canar offers fixed phone lines and home internet. Major internet providers provide 3G services. In December 2014, the Minister of Communications and Information

16 Author’s interview.
17 Net Index “The Global Standard in Internet Metrics.”
Sudan

Technology stated that 4G would be introduced in Sudan mid-2015, though as of June 2015, 4G had not been installed.

Increasing prices on telecom services in 2014-2015 were partially due to tax incentives given to telecom providers alongside higher value added taxes (VAT) imposed on consumers. In 2013, the government of Sudan exempted the telecommunications sector from a 30 percent tax on all profits until the end of 2015. Despite the exemption, the government’s revenue from the telecommunications sector grew in 2014-2015 due to VAT revenues totaling US $600 million per year from consumers, while revenue taxes on telecoms did not exceed US $40 million per year.

Regulatory Bodies

Founded in 1996 and housed under the Ministry of Telecommunications and Information Technology, the National Telecommunications Corporation (NTC) is tasked with producing telecommunications statistics, monitoring the use of the internet, introducing new technology into the country, and developing the country’s telecommunications and IT industry. It is also responsible for deciding what content should be accessible on the internet. Although it is a state body, the NTC receives grants from international organizations such as the Intergovernmental Authority on Development and the World Bank, and its website describes the body as “self-financing.”

Limits on Content

Online self-censorship increased notably in 2014-2015 in response to the government’s heavy-handed crackdown against both print and online media in advance of the April 2015 elections. Government efforts to manipulate the online information landscape also became more concerted and systematic.

Blocking and Filtering

News websites and social media platforms were not blocked in Sudan during the coverage period, though access to Facebook and the online news outlet Al Rakoba was reportedly very slow or at times virtually inaccessible to many users. Meanwhile, Sudanese officials regularly demanded the blocking of online news outlets, particularly after the outlets criticized government officials or published articles about corruption.

The Sudanese government openly acknowledges blocking and filtering websites that it considers “immoral” and “blasphemous.” The NTC manages online filtering in the country through its Internet Service Control Unit and is somewhat transparent about the content it blocks, reporting that 95

---

23 See World Time Zone: http://www.worldtimezone.com/4g.html
27 Author’s interviews.
Sudan

percent of blocked material is related to pornography.\(^{29}\) The NTC’s website also gives users the opportunity to submit requests to either block or unblock websites “that are deemed to not contain pornography,”\(^{30}\) though it does not specify whether the appeals extend to political websites. Users attempting to access a blocked site are met with a black page that explicitly states, “This site has been blocked by the National Telecommunications Corporation,” and includes links to further information and a contact email address.\(^{31}\)

In addition to the NTC, NISS agents reportedly have the technical capability to block websites deemed harmful and threatening to Sudan’s national security,\(^{32}\) while the General Prosecutor also has the right to block any site that threatens national security or violates social mores.\(^{33}\)

During a June 2014 workshop on online media, the Sudanese Information Minister described Facebook and independent online news outlets *Al Rakoba, Hurriyat*, and *Sudanese Online* as “anomalous” and “mercenary” and stated his intention to censor the sites for tarnishing Sudan’s image and blocking potential foreign investment opportunities.\(^{34}\) The minister reiterated the same official position against online media in a televised interview,\(^{35}\) affirming that the government blocks content that it perceives as immoral or a threat to national security.

**Content Removal**

The extent to which the government forces websites to delete certain content is unknown, though anecdotal incidents in 2014-2015 suggested that some degree of forced content removal by the state exists, and that such ad hoc requirements lack transparency. For example, in March 2014, the government forced three news outlets to delete articles from their websites that had cited a government press release, which quoted an official from the ruling National Congress Party (NCP) using an offensive slur to characterize the opposition.\(^{36}\) Criticism of the quote went viral on social media, prompting the NCP—beleaguered by strong pushback from the opposition in the lead up to the April 2015 presidential elections—to delete the original press release from its own website, in addition to forcing other outlets to both delete the stories and post a retraction.\(^{37}\) Furthermore, the NCP dismissed its Khartoum-chapter webmaster from his job for publishing the statement that had caused the social media uproar.\(^{38}\)

**Media, Diversity, and Content Manipulation**

Despite increasing instances of internet censorship in recent years, online newspapers in Sudan con-

---

30 “Blocking Or Unblock Websites.”
32 “Expert: NISS is capable of blocking websites that are posing a threat to Sudan’s national security,” *Aljazeera*, November 7, 2014.
Sudan

tinue to have more freedom than traditional media outlets, which are frequently subject to pre-publication censorship, confiscations of entire press runs of newspapers, and warnings from NISS agents against reporting on certain taboo topics, which include human rights violations linked to the country’s conflict regions, state corruption, the economic recession, and criticism of national security agents.39 Restrictions on print and broadcast news outlets increased following the National Security Act of 2010, which gave the NISS permission to arrest journalists and censor newspapers under the pretext of national security.

Compared to the highly restrictive space in the traditional media sphere, the internet remains a relatively open space for freedom of expression, with bold voices expressing discontent with the government on various online platforms. Many print newspapers circulate censored or banned material on their websites and social media pages, leading Sudanese citizens to increasingly turn to online outlets and social media for uncensored information. Continuous pressure on traditional media has led a number of independent journalists to establish online news outlets in the past few years, though several outlets were subject to frequent technical attacks by government forces throughout 2014-2015 as part of an apparent attempt to limit access to independent news and voices in the lead-up to the April 2015 elections (see “Technical Attacks”).

Blogging is an important platform for journalists and writers to publish commentary free from the restrictions leveled on print newspapers. Blogs also give ethnic, gender, and religious minorities a venue to express themselves. As of mid-2015, there were about 300 Sudanese blogs registered with the Sudanese Bloggers Network. The more active Sudanese bloggers write in the English language.

Nonetheless, online self-censorship increased notably in 2014-2015 in response to the government’s heavy-handed crackdown against both print and online media in advance of the April 2015 elections.40 The majority of journalists writing for online newspapers, such as the newly established Altreeq and Altaghyeer, write anonymously.41

Government efforts to manipulate the online information landscape have become more concerted and systematic. During the coverage period, the government’s Cyber Jihadist Unit continued to spread misinformation on news related to human rights violations and corruption allegations. The unit, which falls under the NISS, proactively monitors content posted on blogs, social media websites, and online newspaper forums and infiltrates online discussions in an effort to ascertain information about cyber-dissidents.

A largescale cyber jihadist campaign was launched in November 2014 in response to global online and offline activism surrounding the mass rape of over 200 women and girls in Tabit town in North Darfur by Sudanese soldiers,42 which was first reported by Radio Dabanga.43 Led by Khalid Ewais, a

40 Author’s interview.
41 Altaghyeer [Arabic for change with political connotation] was established in 2013 following the government’s crackdown on independent journalists, who were eventually banned from practicing traditional journalism in Sudan in 2012. For more, see Reem Abbas, “Sudan’s Shift from Print to Online Newspapers,” Doha Centre for Media Freedom, May 16, 2013, http://bit.ly/1GniAKB. Altreeq was established in January 2014, and its “Who we are” section does not include names of staff but rather the institution’s reporting code of conduct.
43 Launched from the Netherlands in November 2008, Radio Dabanga focuses on reporting on Darfur and has a strong online presence and wide audience in conflicts areas. It website is bilingual and runs in depth reports and features. It is a
Sudan

Sudanese journalist based in the United Arab Emirates, the social media campaign to raise awareness about the mass rape led to several demonstrations around the world and in Sudan. Various counter-campaigns from the Cyber Jihadist Unit were subsequently launched on both government and ostensibly apolitical social media pages that aimed to delegitimize the rape atrocity by smearing Radio Dabanga and Khalid Ewais. For example, cyber jihadists circulated a message on WhatsApp claiming that Ewais had received a US $1 million bribe from the African Union/United Nations Hybrid operation in Darfur (UNAMID), which Ewais denied in an interview with a Khartoum-based newspaper.

In its attempt to distort the facts, cyber jihadists then posted a video on YouTube in which Tabit residents were interviewed denying the Radio Dabanga report. Simultaneously, the government’s “Official Page of the Rapid Response Operations Room” Facebook page published photos showing a women’s rally in Tabit denying the report and claiming that Radio Dabanga had dishonored them. All the while, members of the Sudanese parliament openly demanded the blocking of Radio Dabanga in Sudan. The government eventually yielded to international pressure garnered by the campaign and allowed officials from the United Nations Mission in Darfur (UNAMID) to conduct an investigation, albeit under the government’s supervision. Unfortunately, the government subsequently blocked the investigation and later closed down the UN Human Rights office in Khartoum.

Digital Activism

Despite numerous obstacles and restrictions on ICTs in Sudan, the country’s growing population of technologically savvy citizens regularly engages in digital activism to demand government accountability and social change. Digital activism was particularly vibrant in the lead-up to the April 2015 general elections, as exemplified by the “Leave!” campaign launched in February 2015 in response to President Omar Al-Bashir’s statement that he would not leave the presidency unless he was voted out, which citizens rejected given the Al-Bashir’s record of rigging elections in the past. The campaign encouraged a wholesale boycott of the election as a form of protest against Al-Bashir’s au-

46 Khalid Ibrahim Ewais, Facebook Post, November 23, 2014, http://on.fb.me/1QN8y6i.
Sudan

Though several organizers of the “Leave!” campaign were arrested around the country and Al-Bashir was ultimately re-elected in April, voter turnout stood at between 30-35 percent compared to 72 percent in the previous elections in 2010, reflecting the boycott’s relative success.

Violations of User Rights

A new Freedom of Access to Information Law passed in January 2015 classifies 12 types of information that are restricted from citizens, which observers believe was part of an effort to legalize the government’s censorship powers. In the lead-up to the April 2015 general elections, the government took preemptive measures to restrict critical information and silence the opposition by arresting numerous online journalists and activists. Hacking attacks against critical news websites and activists’ social media accounts also escalated around the general elections.

Legal Environment

Freedom of speech, expression, and association are nominally protected under the 2005 Interim National Constitution (INC) that was adopted as part of the 2005 Comprehensive Peace Agreement (CPA) between the government of Sudan and the southern rebel group, though the constitution officially expired following the independence of South Sudan in July 2011. In January 2015, the parliament approved new amendments to the constitution regarding the elections; however, a permanent constitution is still being developed as of mid-2015, leaving the INC as the country’s highest binding document. Sudan’s judiciary is not independent, though it recently ruled against the government in support of press freedom, reversing a government order to shut down the Al-Tayar independent daily in March 2014.

Sudan has several restrictive laws that seek to limit press and internet freedom. For example, the Informatic Offences (Combating) Act (known as the IT Crime Act, or electronic crimes law), criminalizes the establishment of websites that criticize the government or publish defamatory material and content that disturbs public morality or public order. Violations involve fines and prison sentences between two to five years. The 2009 revisions to the highly restrictive 2004 Press and Printed Press Materials Law allows for restrictions on the press in the interests of national security and public order.

62 Abdelgadir Mohammed Abdelgadir, Fences of Silence: Systematic Repression of Freedom of the Press, Opinion and Expression in Sudan, (International Press Institute, 2012) http://bit.ly/1Pv7nee. According to Section 4, crimes against public order and morality Sudan cyber law, of Sudan’s Cybercrime Law (2007), intentional or unintentional producing, preparing, sending, storing, or promoting any content that violates public order or morality, makes the offender liable to imprisonment of 4 to 5 years or a fine or both. The maximum penalty for committing both crimes is 7 years or fine or both. Also, under the same section, creating, promoting, using, website that calls for, or promote, ideas against public law or morality is punished by 3 years in prison or fine or both. Cyber deformation crimes necessitate 2 years in prison or fine or both. Public order is not defined clearly in the law. Subsequently, most of the opposition content online falls under this section making online activists liable under this law.
Sudan

and holds editors-in-chief liable for all content published in their newspapers.\textsuperscript{63} The 2010 National Security Act gives the NISS immunity from prosecution and the permission to arrest, detain, and censor newspapers under the pretext of national security.\textsuperscript{64} Though there are no specific references to online media, the press and national security laws' broad wording allows them to be applied to online content.

In January 2015, the government passed a new Freedom of Access to Information Law\textsuperscript{65} with the supposed aim of improving Sudan's last place ranking on Transparency International's Corruption Perceptions Index.\textsuperscript{66} While the government claimed that the law would increase transparency and the public's access to information,\textsuperscript{67} the law itself has not been made publicly available as of mid-2015. According to local reports and observers, the law is in practice highly limiting, with provisions that reportedly classify 12 types of information that are restricted from citizens, such as national security and foreign policy information, among others.\textsuperscript{68} The classification system effectively leaves no room for journalists or the public to access any information of consequence. Moreover, freedom of information requests will be overseen by a minister appointed by the president, giving the executive branch exclusive control over access to information, while arbitrarily determined fees imposed for each inquiry will make the process of requesting information burdensome. Furthermore, according to local sources, individuals will be perversely subject to penalties under other laws if they request certain types of classified information, such as information that the government could decide is a threat to national security.\textsuperscript{69} Many observers believe the government passed the new law to legalize the withholding of information and its censorship powers.\textsuperscript{70} Others contend the law provides the legal grounds to argue for more access to information.\textsuperscript{71}

Meanwhile, a new draft press law introduced in December 2012 is still in the works as of mid-2015. According to a statement by the head of the Press and Publications Council in November 2014, the new press law will include sections governing online journalism.\textsuperscript{72} Also in November 2014, the Sudanese police department stated that it had over 200 cybercrime cases open against 250 defendants during 2014, which the authorities used as an argument for including online journalism in the new press law.\textsuperscript{73} Activists believe that the government exaggerated the number of cybercrime cases to justify passing more restrictive laws to regulate the internet.

Online journalists have no legal status in Sudan.\textsuperscript{74} While this legal limbo can be beneficial for online

\textsuperscript{66} International Transparency, “Sudan visualization,” http://www.transparency.org/country#SDN.
\textsuperscript{68} Other classified information restricted from access: confidential documents; national defense secrets; information about laws in process; personal information such as education, profession, and finance; personal correspondence; information that could affect ongoing negotiations; information related to police investigations or judicial committees; confidential political information; and information that is scheduled to be public. See: “Government classifies 12 types of information and charges fees obtain the information,”[in Arabic] Alyoum Altai, January 19, 2015, http://bit.ly/1RSO875.
\textsuperscript{69} According to Freedom House interviews with an anonymous Sudanese journalist, March 2015.
\textsuperscript{70} Author's interview, March 2015.
\textsuperscript{71} Author's interview, March 2015.
\textsuperscript{72} “Expert: NISS is capable of blocking websites that are posing a threat to Sudan’s national security.”
\textsuperscript{73} “Police: Increase in cybercrimes in the country,” Alyoum Altai, November 7, 2014.
Sudan

journalists, freeing them from the limitations of the restrictive press law, they forfeit many privileges available to print journalists, such as media access at official events.75

Prosecutions and Detentions for Online Activities

In the lead-up to the April 2015 general elections, the government took preemptive measures to restrict critical information and silence the opposition by arresting online journalists and activists:

- In December 2014, police detained Altayyar journalist Tagelsir Wadelhkhair for publishing on the newspaper’s website a story about real estate corruption that involved the senior legal advisor to the Ministry of Justice and the former director of the Land Registry Office.76 He was held for one day and charged with defamation.

- In May 2015, online female activist Solafa Saad was arrested by plainclothes security services following a Facebook post describing her personal experience with racism, which was widely disseminated.77 She was interrogated for seven hours, during which her interrogators blamed her for the wide circulation of her Facebook post. The interrogators were particularly furious that her post was picked up by the satirical Facebook page “Al-Bashir Diary.”78 Saad was beaten by her interrogators, who used racial slurs and shaved her head for talking back at them.79

- In July 2015, Waleed Al Hussein, the creator of the critical online news outlet, Al Rakoba, was arrested by the authorities in Saudi Arabia, where he had been residing with his family.80 As of September, he was being held in solitary confinement without charges and subjected to interrogations about his work with Al Rakoba. Family members believe he was arrested at the request of the Sudanese government, which had targeted Hussein for his work in the past and was seeking to have him extradited back to Sudan.81

Surveillance, Privacy, and Anonymity

Unchecked surveillance of ICTs is a grave concern in Sudan. The Sudanese government actively monitors internet communications on social media platforms, particularly targeting online activists and journalists during political protests, and the NISS regularly intercepts private email messages, enabled by sophisticated surveillance technologies.

According to Citizen Lab research from June 2013, Sudan possesses high-tech surveillance equipment from the U.S.-based Blue Coat Systems, a technology company that manufactures monitoring and filtering devices. The surveillance system was initially traced to three networks inside Sudan, in-

---

75 Author’s interview, March 2015.
77 Solafa Saad, Facebook Post, April 30, 2015, http://on.fb.me/1NRKygr.
79 Retrieved from the activist Facebook account - her status was set to public. Solafa Saad, Facebook Post, April 30, 2015, http://on.fb.me/1NRKygr.
Sudan

including on the networks of the private telecom provider Canar. In addition, Citizen Lab also located sophisticated computer spyware technology known as Remote Control System (RCS) by the Italian company Hacking Team in Sudan in early 2014. Advertised by Hacking Team as “offensive technology” sold exclusively to law enforcement and intelligence agencies around the world, RCS spyware has the ability to steal files and passwords and intercept Skype calls and chats. Internal emails leaked by hackers in July 2015 confirmed that Sudan’s NISS had purchased Hacking Team’s RCS spyware in 2012, though another leaked email from January 2014 revealed that training of intelligence agents was stymied by an overwhelming lack of computer literacy and English-language skills. Other leaked emails revealed that the company had discontinued business with Sudan in November 2014.

Use of mobile phones has become increasingly dangerous for activists, given widespread suspicion that the authorities possess phone-tapping and location tracking tools. A number of Sudanese journalists and activists have reported fears that their phones are tapped, and there is a strong belief among Sudanese activists and journalists that the government has advanced capabilities to remotely activate a mobile phone’s microphone to eavesdrop on conversations even if the cell phone is switched off. According to anonymous sources, the Iranian Ambassador once requested journalists to place their inactive cell phones far away from their conversation with the Ambassador, who had admitted that they [the Iranians] themselves had introduced this capability to the Sudanese government.

SIM card registration requirements were enacted in 2008, compromising mobile phone users’ privacy and anonymity, particularly given the strong sense among observers that the government is able to access user communications through providers without due process. In a renewed effort to enforce SIM card registration—which requires an official identification card and home address information—the government disconnected all unregistered SIM cards in June 2014 and reportedly plans to link SIM cards to users’ national identification numbers in the future.

Intimidation and Violence

Security agents in Sudan regularly employ extralegal intimidation, harassment, and violence against online journalists and activists. The authorities also routinely abuse political detainees to obtain access to private communications that could be used as evidence in court. In one case from Sep-

85 PDF of a receipt that shows the National Intelligence and Security Services of Sudan purchased Hacking Team’s services: http://bit.ly/1Pv9A9p.
88 Interview in Khartoum, Sudan, August 1, 2012.
90 Author’s interview, March 2015.
91 Freedom House interview, March 2015.
94 “Sudan: Telecoms companies block non-registered SIM cards.”
Sudan

tember 2014 reported by the Sudanese Human Rights Network, NISS officials used torture to force a political detainee to reveal his email passwords.95

Sudanese women are regularly targeted for harassment and cyberbullying by both state and non-state actors for their online activities. Throughout 2014-2015, numerous female bloggers received online threats for activities that ranged from sharing their views on wearing the hijab to writing feminist poetry.96 There were also reports of security agents arbitrarily detaining female online activists for periods between seven hours and three days on spurious charges of defamation and spreading rumors.

Technical Attacks

Independent online news outlets are frequently subject to hacking attacks by what activists believe is the work of the Cyber Jihadist Unit. A group calling itself Haras al Hudoud (“soldiers of the frontier”) also claimed responsibility for several technical attacks throughout the year,97 advertising itself on screen when users tried to access hacked sites while they were down.98 Some online newspapers reported hacking attempts traced to hackers in India and Sudan.99

Several cyberattacks against critical news websites and activists’ social media accounts occurred during the coverage period, escalating around the April 2015 general elections:

- The website of Nuba Reports, which provides in-depth coverage of ongoing conflicts in Sudan’s war-torn regions, was hit in September 2014 with a massive DDoS attack. The attack came three days after a Nuba Reports summary of human rights violations in the conflict regions since 2012 was circulated at the 27th session of the UN Human Rights Council in Geneva.100 Since then, the site has been under constant attack.101

- In October 2014, during the campaign to raise awareness about the mass rape of 200 women in South Darfur, campaign leader Khalid Ewais’s Facebook account was hacked a number of times, leaving it disabled for five days in a row during one of the attacks.102

- In November 2014, independent outlet Alrakoba was hacked by Haras al Hudoud and was offline for a day.

- On April 12, 2015, the eve of national elections in Sudan, online news outlets SudaNile and Hurriyat experienced simultaneous Denial of Service (DoS) attacks. The outlet 3ayin was attacked two days later. Consequently, two of the websites were disabled for over ten hours, while SudaNile was down for five consecutive days.

---

96 Author interviews. “Hijab is a head covering worn in public by some Muslim women” Oxford Dictionary. Sudanese Public Order Law orders that women wear head cover when they are in public space.
97 “Haras al Hudoud refers to a group of the government’s armed forces in Darfur, though there is no direct evidence that the government was behind the hacking attack.” See Freedom House, “Sudan,” Freedom on the Net 2014.
99 Author’s interview.
102 Author’s interview.
Sudan

Facebook user Wad Galuba, who posts news about corruption and insiders insights of NISS operations, reported frequent hacking attempts and death threats every time the user published a hot topic.104

International experts and commentators on Sudan also reported massive, and repeated, attacks on their online accounts.105

---

104 Author’s interview.
Key Developments: June 2014 – May 2015

- The war has devastated telecommunications infrastructure and disconnected around two-thirds of the country from Syrian internet service providers. As a result, internet access has become highly decentralized with some relying on microwave links from Turkish cities or satellite connections serving cybercafes (See Availability and Ease of Access).

- At least 12 activists, bloggers, and citizen journalists were killed over the past year by both the regime and rebel forces, including the Islamic State. Blogger Assad Hanna left Syria following online threats stemming from his criticism of the regime, but was badly injured by knife-wielding assailants at his apartment in Turkey (see Intimidation and Violence).

- Hackers affiliated with or supportive of the Islamic State have stepped up cyberattacks of Syrian citizen journalists or groups documenting human rights abuses, while the progovernment Syrian Electronic Army continues to target Western media outlets (see Technical Attacks).
Introduction

Syria remained one of the most repressive and dangerous environments for internet users in 2015. Syrian cyberspace remains fraught with conflict, often mirroring the brutality of the war on the ground. Authorities employ sophisticated technologies to filter political, social, and religious websites, and to conduct surveillance on citizens. Phishing, spear-phishing, malware, DDoS and other cyberattacks have grown dramatically over the past two years. This year, progovernment hackers have shifted tactics, now carrying out targeted attacks against Syrian opposition members or journalists, as well as operations against foreign websites. The aim of these attacks has been to gain sensitive information about opposition networks or reporters. Individuals are regularly detained and tortured for their online posts or digital activism, either by the Syrian government or by armed extremists such as the Islamic State of Iraq and the Levant (IS), whose power has increased over the past years. The situation for bloggers, journalists, and citizen journalists has only grown worse as a result; Syria recorded the highest number of deaths of citizen journalists in the world. Nonetheless, despite weak infrastructure, online restrictions, and harsh punishments for online activities, Syrians have made extensive use of social networks and online tools to document human rights abuses and mobilize protests.

The internet was first introduced to Syria in 2000, immediately after the transfer of power from Hafez al-Assad to his son, current president Bashar al-Assad. The internet came to portray the new president’s ostensible emphasis on modernity and evolution. Inspired by regional events, a civic protest movement began in February 2011, calling for political reforms, the end of emergency rule, and basic freedoms. By early 2012, after brutal crackdowns on demonstrations in several cities, events descended into armed conflict. Authorities prevented foreign media from accessing the situation on the ground, prompting many ordinary Syrians to take up mobile phones and small cameras to cover the deteriorating situation and post videos on social media. These citizen journalists have become vital in the quest to document flagrant human rights abuses by all parties to the conflict.

Since the start of the conflict, government censorship and retaliation against internet users has intensified. Tactics have included periodic shutdowns of internet and mobile phone service, increased filtering of websites, sophisticated monitoring of users’ online activities, as well as the confiscation of laptops, mobile phones, and other equipment used by citizen journalists. Shelling and sabotage have led to heavy damage to infrastructure, affecting internet and power connections in seven provinces. The poor state of internet service has led many opposition activists to use satellite connections, which can be tracked easily and have resulted in targeted bombings against media centers, as occurred in the 2012 death of journalist Marie Colvin. Combined, these developments make Syria one of the worst countries for internet freedom in 2014-15.

Obstacles to Access

The war has devastated telecommunications infrastructure and disconnected around two-thirds of the country from Syrian internet service providers (ISPs). As a result, internet access has become highly decentralized with some relying on WiMax microwave links from Turkish cities or pooled satellite connections serving cybercafes.

Availability and Ease of Access

Syria's telecommunications infrastructure is one of the least developed in the Middle East, with broadband connections among the most difficult and expensive to acquire. This worsened after 2011, as inflation and electricity outages increased dramatically following public protests and the government's corresponding crackdown. Damage to the communications infrastructure was particularly bad in the cities of Der Azzor, Aleppo, and al-Hasakah, as they were subject to severe shelling by both the Syrian armed forces and the opposition. This has led to a decentralized telecommunications infrastructure, whereby each and every part of the country has a different gateway to access.

By the end of 2014, the International Telecommunication Union reported that 28 percent of Syrians had access to the internet, up from 17 percent in 2009. The number of fixed broadband subscribers remains small at 1.68 subscriptions per 100 inhabitants, while mobile phone penetration was 71 percent, up from 56 percent last year.

The price, speed, and availability of internet access vary depending on the region of the country. According to a pricelist published by the Ministry of Communication and Technology, the monthly cost for 1 Mbps connection was SYP 1400 (approximately US$5) as of April 2015, in a country where monthly gross domestic product per capita was US$274. While the Syrian lira (SYP) has lost a large amount of its value, prices have not changed dramatically over the conflict. However, around two-thirds of the country is disconnected from Syrian ISP networks, instead relying on a WiMax microwave link from Turkish cities or on satellite connections (VSAT). The former is prominent in Kurdish areas along the Turkish border, such as Qamishli, resulting in Wi-Fi connections of around US$80 per month. Due to the prohibitive cost of VSAT connections, businesses in IS-controlled areas have established cybercafes where users split the cost of satellite infrastructure and purchase separate Wi-Fi connectivity. Based on Skype interviews with Syrians living under IS-controlled areas, the cost of buying a Wi-Fi access point is around SYP 5,000 (US$17), granting 64Kbps speeds and data at SYP 400 ($1.25) per 100 MB. IS recently required cybercafes to obtain a license in order to operate.

Furthermore, in mid-2015, IS released a statement requiring these cybercafes to "remove Wi-Fi boosters in internet cafes as well as private wireless adapters, even for soldiers of the Islamic State." The move is an attempt to limit private internet access in Raqqa and Deir Ezzor to public locations that can be policed by the extremists in order to restrict reporting by activists as well as GPS-tracking of militants using the services.

---

6 " Northern Syria, Internet cafes are everywhere in the North, Chatting, Smoking and Porn," [in Arabic], Hunassootak, http://bit.ly/1Q4ieBU.
8 Interview with Abu Ibrahim Raqqawi of Raqqa Is Being Slaughtered Silently, Skype.
Syria

Restrictions on Connectivity

The country’s connection to the international internet remains centralized and tightly controlled by the government. This centralization has contributed to connectivity problems, as the weak and overburdened infrastructure often results in slow speeds and periodic outages. In addition to its regulatory role, the Syrian Telecommunications Establishment (STE), also serves as an ISP. Private ISPs like Aya, as well as mobile phone internet providers, are required to sign a memorandum of understanding to connect via the gateways controlled by the Syrian Information Organization (SIO).

During late 2014 and early 2015, the Syrian government continued to obstruct connectivity through its control of key infrastructure, at times shutting down the internet and mobile phone networks entirely or at particular sites of unrest. Since January 2014, Syrians in Deir ez-Zor, Qamishli, and other cities faced a full internet blackout, mainly due to destroyed infrastructure. In other areas, many speculate outages are timed to coincide with a specific political or military purpose. Two shutdowns occurred in November and December 2012. More localized, but longer lasting cut-offs were reported in seven provinces all across the country. This includes, for example, a full shutdown in Aleppo on August 11, 2012.

ICT Market

The total number of Syrian ISPs was at 14 as of 2012. Independent satellite connections are prohibited, although in reality, they are heavily employed due to the unreliability of government ICT infrastructure. ISPs and cybercafes must obtain approval from the STE and pass security vetting by the Ministry of Interior and other security services. Moreover, cybercafe owners are required to monitor visitors and record their activities. There are two main mobile phone providers in Syria: Syriatel—owned by Rami Makhlouf, a cousin of President Bashar al-Assad—and MTN Syria, a subsidiary of the South African company.

Regulatory Bodies

Syria’s ICT market and internet policy is regulated by the SIO and the state-owned STE, which owns

---

all fixed-line infrastructures. The STE is a government body established in 1975 as part of the Ministry of Telecommunications and Technology.\(^\text{20}\)

### Limits on Content

The Syrian government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs. Self-censorship is highly prevalent, particularly in areas under government control. Despite these limitations, citizen journalists continue to make use of video-uploading sites and social networks to spread information about human rights abuses and the atrocities of war. Their role has become particularly important at a time when traditional journalists operate in highly unsafe conditions and foreign press visas are difficult to obtain.

### Blocking and Filtering

In recent years, censorship has expanded; the blocking of websites related to government opposition, human rights groups, the Muslim Brotherhood, and activism on behalf of the Kurdish minority is very common.\(^\text{21}\) A range of websites related to regional politics are also inaccessible, including the prominent London-based news outlets *Al-Quds al-Arabi* and *Asharq al-Awsat*, as well as several Lebanese online newspapers and other websites campaigning to end Syrian influence in Lebanon. Access to the entire Israeli top-level domain "\(\text{.il}\)" was also restricted. However, the websites of most international news sources and human rights groups have remained accessible.

Censorship is implemented by the STE and private ISPs with the use of various commercially available software programs. Independent reports in recent years pointed to the use of ThunderCache software, which is capable of “monitoring and controlling a user’s dynamic web-based activities as well as conducting deep packet inspection.”\(^\text{22}\) In 2011, evidence emerged that the Syrian authorities were also using technology provided by the Italian company Area SpA to improve their censorship and surveillance abilities. The contract with Area SpA included software and hardware manufactured by companies such as Blue Coat Systems, NetApp, and Sophos. Blue Coat had reportedly sold 14 devices to an intermediary in Dubai which then sent them to Area SpA, ostensibly with Blue Coat believing that the equipment would be given to the Iraqi government; however, logs obtained by the hacktivist group Telecomix in August 2011 revealed evidence of their use in Syria instead.\(^\text{23}\) In October of that year, Blue Coat acknowledged that 13 of the 14 devices had been redirected to the Syrian government, an inadvertent violation of a U.S. trade embargo, and that the company was cooperating with the relevant investigations.\(^\text{24}\) Analysis of the exposed Blue Coat logs revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites.\(^\text{25}\) The *Wall Street Journal* identified efforts to block or monitor tens of thousands of opposition

---

websites or online forums covering the uprising. Out of a sample of 2,500 attempts to visit Facebook, the logs revealed that three-fifths were blocked and two-fifths were permitted but recorded.\footnote{Jennifer Valentino-Devries, Paul Sonne, and Nour Malas, "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web,” Wall Street Journal, October 29, 2011, http://on.wsj.com/t6YI3W.}

The Syrian government also engages in filtering mobile phone text messages. Beginning in February 2011, such censorship was periodically reported around dates of planned protests. In February 2012, the news service Bloomberg reported that a series of interviews and leaked documents revealed that a special government unit known as Branch 225 had ordered Syriatel and MTN Syria to block text messages containing key words like “revolution” or “demonstration.” The providers reportedly implemented the directives with the help of technology purchased from two separate Irish firms several years earlier for the alleged purpose of restricting spam.\footnote{Ben Elgin and Vernon Silver, “Syria Disrupts Text Messages of Protesters With Dublin-Made Equipment,” BloombergBusiness, February 14, 2012, http://bloom.bg/1i0TOEU.}

The government continues to block circumvention tools, internet security software, and applications that enable anonymous communications. By enabling deep packet inspection (DPI) filtering on the Syrian network, authorities were able to block secure communications tools such as OpenVPN, Later 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPsec) in August 2011.\footnote{Dlshad Othman, “Bypassing censorship by using obfsproxy and openVPN, SSH Tunnel,” Dlshad, June 22, 2013, http://bit.ly/1KH3KjZ.} Websites used to mobilize people for protests or resistance against the regime, including pages linked to the network of Local Coordination Committees (LCCs)—groups that have formed since the revolution to organize the opposition—continue to be blocked.\footnote{Local Coordination Committees, “Home,” http://www.lccsyria.org/en/.} Websites that document human rights violations, such as the Violations Documentation Center, remain blocked,\footnote{“Leaked list of all blocked websites in Syria,” Arab Crunch, May 19, 2013, http://bit.ly/1KGFP8m.} as does the Mondaseh website, an online initiative to gather information and raise public awareness.\footnote{“Home,” the-syrian, http://english.the-syrian.com/} Authorities have repeatedly blocked the website and key search terms of SouriaLi, an internet radio station started by a group of pluralistic young Syrians.\footnote{Syria Untold, “Syrian Creativity: Radio SouriaLi Broadcasts over the Internet,” Global Voices, June 7, 2013, http://bit.ly/1EQQ2ZS.}

Facebook remains accessible in Syria after the government lifted a four-year block on the social-networking site in February 2011. Nonetheless, according to one Damascus-based activist, Facebook pages sometimes do not load correctly and display a Transmissions Control Protocol (TCP) error message. The video-sharing website YouTube was also unblocked, although it was not usable from mobile phone devices due to limits on data speeds.\footnote{Interview with activist requesting anonymity, December 2011, Syria.} Some activists suspected, however, that rather than a sign of openness, the regime’s motive for unblocking the sites was to track citizens’ online activities and identities. As of March 2012, both were within the top-five most visited websites in the country. More recently, neither of the sites appear in the Top 25, perhaps due to users employing proxies that change their IP address to another country.\footnote{Alexa, “Top Sites in SY,” accessed August 14, 2012, http://www.alexa.com/topsites/countries/SY.} Other social media platforms like Twitter are freely available, although the presence of Syrian users on them is minimal.

Despite the free access to Facebook and YouTube, a range of other social media applications remain inaccessible in Syria. The Voice over Internet Protocol (VoIP) service Skype often suffers from disruptions either due to low speeds or intermittent blocking by the authorities. In February 2012, the gov-
ernment also began restricting access to certain applications for mobile phone devices that activists had been using to circumvent other blocks. Additionally, other applications reportedly blocked were the live video-streaming service Bambuser, and WhatsApp, an application that allows users to send mobile phone text messages via the internet. Instant messenger services such as eBuddy, Nimbuzz, and mig33 have been disabled by blocking the SMS that users must receive in order to activate their accounts. In other cases, certain online services—such as Google Maps or the photo-sharing tool Picasa—have been rendered inaccessible from Syria by their U.S.-based service providers due to restrictions related to economic sanctions against the country. More applications, such as anti-virus software and updates to operating systems, remain blocked by sanctions, pushing many U.S.-based activists to ask for a reevaluation of the sanctions strategy.

Decisions surrounding online censorship lack transparency and ISPs do not publicize the details of how blocking is implemented or which websites are banned, though government officials have publicly admitted engaging in internet censorship. When a user seeks to access a blocked website, an error message appears implying a technical problem rather than deliberate government restriction. Decisions on which websites or keywords should be censored are made by parts of the security apparatus, including Branch 225, or by the executive branch.

Content Removal

Controversially, both Facebook and YouTube have removed content related to the Syrian uprising under the justification that content posted to certain users’ accounts promotes violence or contains graphic content. According to digital security NGO SecDev, dozens of opposition pages, media centers, and independent NGOs have been closed by Facebook. These include numerous pages of LCCs and the London-based Syrian Network for Human Rights. Activists believe that Facebook users sympathetic to President Assad may be reporting the pages as violating user guidelines en masse, thereby provoking Facebook into action. One activist, Razan Zaitouneh of the Violations Documentation Center, shared a letter urging Facebook to keep the sites open, stating that “Facebook pages are the only outlet that allows Syrians and media activists to convey the events and atrocities to the world.” Representatives from Facebook have cited the difficulties in discerning between objective reporting and propaganda, particularly since many armed extremists have taken to using the site.

Media, Diversity, and Content Manipulation

In an environment of extreme violence and arbitrary “red lines,” self-censorship is widespread. Sensitive topics include criticizing President Assad, his late father, the military, or the ruling Baath party. Publicizing problems faced by religious and ethnic minorities or corruption allegations related to

Syria

the ruling family, such as those of Assad’s cousin Rami Makhlouf, are also off limits. Most Syrian users are careful not only to avoid such sensitive topics when writing online, but also to avoid visiting blocked websites. However, the period of May 2012 to April 2013 witnessed a large number of local Syrian users expressing opposition to Assad, his father, Makhlouf, the Baath party, and certain ethnic or sectarian groups. In 2014, users living in areas under control of IS or other extremist groups have stepped up their self-censorship in order to avoid criticizing the militants or Islam.

Pro-regime forces have employed a range of tactics to manipulate online content and discredit news reports or those posting them, though it is often difficult to directly link those who are carrying out these activities with the government. Most notable has been the emergence of the Syrian Electronic Army (SEA), a progovernment hacktivist group that targets the websites of opposition forces, human rights websites, and even Western media outlets (see “Technical Attacks”). For news websites and other online forums based in the country, it is common for writers to receive phone calls from government officials offering “directions” on how to cover particular events. The Syrian government also pursues a policy of supporting and promoting websites that publish progovernment materials in an attempt to popularize the state’s version of events. These sites typically cite the reporting of the official state news agency SANA, with the same exact wording often evident across multiple websites. Interestingly, in 2012, the progovernment website Aksalser changed its stance to support the opposition and was subsequently blocked by the government. Since early 2011, this approach has also been used to promote the government’s perspective about the uprising and subsequent military campaign.

U.S. sanctions have resulted in the blocking of paid online services, making it difficult for Syrians to purchase a domain or host their websites in places like the United States or Europe. Restrictions on importing funds into Syria have had a significant impact on the ability to publish content. For instance, recently, the website of the Syrian magazine Syrian Oxygen attempted to buy SSL certificates for their website. However, they were not able to obtain the certificates from U.S. providers as the domain syrianoxygen.com has the word Syria in it.

Digital Activism

Online tools have proven crucial for Syrians in and outside the country seeking to document human rights abuses, campaign for the release of imprisoned activists, and disseminate news from the front lines of the conflict. Syrians are very active on Facebook, using it as a platform to share news, discuss events, release statements, and coordinate both online and offline activities. A Facebook petition for the release of Youssef Abdelke, initiated by a group of Syrian intellectuals and artists, was signed by over 2,500 users. Abdelke, an illustrator and painter who has often expressed political dissent through his art, was arrested in July 2013 after he signed a declaration, posted online, which called

---

40 Email communication from a Syrian blogger. Name was hidden.
41 Interview with a Syrian activist, November 2012, Damascus, November 2012.
Syria

for a democratic transition and the stepping down of President Assad.\textsuperscript{47} He was released one month later.\textsuperscript{48}

In addition, one observer has called the conflict in Syria the first “YouTube War” due to the extraordinarily high coverage of human rights violations, military battles, and post-conflict devastation that is contained in videos posted to the site.\textsuperscript{49} Indeed, as the Syrian government shifted to the use of heavy arms and missiles against opposition fighters, the role of citizen journalists has shifted from live event coverage to documenting the bloody aftermath of an attack. Hundreds of thousands of videos have been posted to YouTube by citizen journalists, rebel groups, and civil society groups, mostly documenting attacks. A Syrian group categorizing YouTube videos and sharing them via the platform OnSyria had posted almost 200,000 videos in 2013.\textsuperscript{50} Although many obstacles stand in the way of media coverage, citizen journalists have designed techniques to ensure media coverage of remote and conflict areas. “Local Media Offices” ensure that local journalists cover limited geographic areas, and then use a social network as a platform to collect, verify, and publish news stories.

Violations of User Rights

Syria’s constitution provides for freedom of opinion and expression, but these are severely restricted in practice, both online and offline. Furthermore, a handful of laws are used to prosecute online users who express their opposition to the government. Citizen journalists and YouTube users are detained and often tortured by both government forces and, increasingly, fighters linked to extremist groups such as Islamic State. Surveillance tools are used to identify and harass those who oppose the Assad government, often through targeted malware attacks against their computer systems and online accounts. Finally, the websites of opposition groups and human rights organizations are consistently targeted with cyberattacks from hackers linked to the government.

Legal Environment

Laws such as the penal code, the 1963 State of Emergency Law, and the 2001 Press Law are used to control traditional media and arrest journalists or internet users based on vaguely worded terms such as threatening “national unity” or “publishing false news that may weaken national sentiment.”\textsuperscript{51} Defamation offenses are punishable by up to one year in prison if comments target the president and up to six months in prison for libel against other government officials, including judges, the military, or civil servants.\textsuperscript{52} In addition, Syria’s cybercrime law allows prison sentences of up to three years and fines of up to SY$ 250,000 (US$ 1,500) for anyone who incites or promotes crime through computer networks.\textsuperscript{53} The judiciary lacks independence and its decisions are often arbitrary. Some civilians have been tried before military courts.

\textsuperscript{47} “Déclaration pour Syrie democratique” [Declaration for a Democratic Syria], Babelmed, accessed March 14, 2014, \url{http://bit.ly/1zKKHU}.
\textsuperscript{50} The platform, \url{http://onsyria.org/}, is now offline and the related Facebook page has not been updated since 2013: Onsyria, Facebook Page, \url{http://on.fb.me/1GnVymR}.
\textsuperscript{51} Syrian Penal Code, art. 285, 286, 287.
\textsuperscript{52} Syrian Penal Code, art. 378.
Prosecutions and Detentions for Online Activities

Since antigovernment protests broke out in February 2011, the authorities have detained hundreds of internet users, including several well-known bloggers and citizen journalists. While it is very difficult to obtain information on recent arrests, 17 netizens remain in prison according to Reporters Without Borders. 54 Many of those targeted are not known for their political activism, so the reason for their arrest is often unclear. This arbitrariness has raised fears that users could be arrested at any time for even the simplest online activities—posting on a blog, tweeting, commenting on Facebook, sharing a photo, or uploading a video—if it is perceived to threaten the regime’s control. Veteran blogger Ahmad Abu al-Khair was taken into custody in February 2011 while traveling from Damascus to Banias and was later released, though he has remained in hiding. 55 More recently, in an effort to pressure al-Khair to turn himself in, security forces have twice detained his brother, once for a period of 60 days. 56 Bassel Khartabil, an open source activist and recipient of the 2013 Index on Censorship Digital Freedom Award, remains in prison after he was taken by authorities without explanation in March 2012. 57

Human rights activists who work online are also targeted by the government and the rebels. Four members of the Violations Documentation Center (VDC) were kidnapped by an unknown group from a rebel-controlled area in December 2013. 58 Authorities raided the offices of the Syrian Center for Media and Freedom of Expression (SCM) in February 2012, arresting 14 employees. 59 One SCM member and civil rights blogger, Razan Ghazzawi, 60 was detained for 22 days. 61 Three others remain in prison and face up to 15 years for “publicizing terrorist acts” due to their role in documenting human rights violations by the Syrian regime. 62 The organization’s founder and director, Mazen Darwish, was reportedly released in August 2015 after three years in pretrial detention. 63 His hearing had been rescheduled 24 times since 2013. 64

Surveillance, Privacy, and Anonymity

Surveillance is rampant on Syrian internet service providers, which are tightly aligned with security forces. Meanwhile, in IS-controlled territory, there are reports that militants have conducted unannounced raids at cybercafes in which they force users to leave their machines, going through their open web browsing sessions and social media accounts to ensure users are not viewing or writing impermissible content. 65

56 Email communication with activist who wished to remain anonymous, April 2012, Syria.
61 An interview with Syrian blogger, February 2013, Skype.
65 Interview with Abu Ibrahim Raqqawi of Raqqa Is Being Slaughtered Silently, Skype.
Syria

The Law for the Regulation of Network Communication against Cyber Crime, passed in February 2012, requires websites to clearly publish the names and details of the owners and administrators. The owner of a website or online platform is also required “to save a copy of their content and traffic data to allow verification of the identity of persons who contribute content on the network” for a period of time to be determined by the government. Failure to comply may cause the website to be blocked and is punishable by a fine of SYP 100,000 to 500,000 (US$1,700 to $8,600). If the violation is found to have been deliberate, the website owner or administrator may face punishment of three months to two years imprisonment as well as a fine of SYP 200,000 to 1 million (US$1,500 to $7,500). In early 2014, however, the authorities were not vigorously enforcing these regulations.

In early November 2011, Bloomberg reported that in 2009 the Syrian government had contracted Area SpA to equip them with an upgraded system that would enable interception, scanning, and cataloging of all email, internet, and mobile phone communication flowing in and out of the country. According to the report, throughout 2011, employees of Area SpA had visited Syria and began setting up the system to monitor user communications in near real-time, alongside graphics mapping users’ contacts. The exposé sparked protests in Italy and, a few weeks after the revelations, Area SpA announced that it would not be completing the project. No update is available on the project’s status or whether any of the equipment is now operational.

One indication that the Syrian authorities were potentially seeking an alternative to the incomplete Italian-made surveillance system were reports of sophisticated phishing and malware attacks targeting online activists that emerged in February 2012. The U.S.-based Electronic Frontier Foundation (EFF) reported that malware called “Darkcomet RAT” (Remote Access Tool) and “Xtreme RAT” had been found on activists’ computers and were capable of capturing webcam activity, logging keystrokes, stealing passwords, and more. Both applications sent the data back to the same IP address in Syria and were circulated via email and instant messaging programs. Later, EFF reported the appearance of a fake YouTube channel carrying Syrian opposition videos that requested users’ login information and prompted them to download an update to Adobe Flash, which was in fact a malware program that enabled data to be stolen from their computer. Upon its discovery, the fake site was taken down. Due to the prevailing need for circumvention and encryption tools among activists and other opposition members, Syrian authorities have developed fake Skype encryption tools and a fake VPN application, both containing harmful Trojans.

A report from Kaspersky Labs, published in August 2014, revealed that some 10,000 victims’ computers had been infected with RATS in Syria, as well as in other Middle Eastern countries and the

---

66 *Law of the rulers to communicate on the network and the fight against cyber crime* art. 5-12. Informal English translation: [https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html](https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html).
67 *Law of the rulers to communicate on the network and the fight against cyber crime* art. 2.
68 *Law of the rulers to communicate on the network and the fight against cyber crime* art. 8.
71 Ben Brumfield, “Computer spyware is newest weapon in Syrian conflict,” CNN, February 17, 2012, [http://cnn.it/1LZPOXt](http://cnn.it/1LZPOXt).
74 Syrian Malware” Up-to-date website collecting the malware [http://syrianmalware.com/](http://syrianmalware.com/).
United States. The attackers sent messages via Skype, Facebook, and YouTube to dupe victims into downloading surveillance malware. One file was disguised as a spreadsheet listing names of activists and “wanted” individuals.

Anonymous communication is possible online but increasingly restricted. Registration is required to purchase a cell phone, though over the past years, activists have begun using the SIM cards of friends and colleagues killed in clashes with security forces in order to shield their identities. Cell phones from neighboring countries like Turkey and Lebanon have been widely used since 2012, notably by Free Syrian Army fighters. However, civilians in Syria are now also using these foreign cell phones due to the lack of cell service in the country. Meanwhile, activists and bloggers released from custody report being pressured by security agents to provide the passwords of their Facebook, Gmail, Skype, and other online accounts.

Intimidation and Violence

Once in custody, citizen journalists, bloggers, and other detainees reportedly suffered severe torture on behalf of government authorities. Although the precise number is unknown, it is estimated that dozens of individuals have been tortured to death for filming protests or abuses and then uploading them to YouTube. In some cases around the country, the Syrian army appeared to deliberately target online activists and photographers. In response to such brutality, hundreds of activists have gone into hiding and dozens have fled the country, fearing that arrest may not only mean prison, but also death under torture. Blogger Assad Hanna left Syria following online threats stemming from his criticism of the regime, but was badly injured by knife-wielding assailants at his apartment in Turkey.

Attacks on activists and citizen journalists were not limited to Syrian government forces. The Free Syrian Army (FSA), the opposition armed movement, have committed many attacks on videographers and citizen journalists, mainly in the suburbs of Aleppo. Since the “liberation” of Aleppo province, some activists and photographers have complained of being targeted by FSA fighters more than they were targeted by the Syrian government, according to one anonymous source in the region.

Further, the Al Nusra Front (Jabhat al Nusra), a group of armed extremists, have arrested tens of young citizen journalists for weeks at a time, and in one incident, opened fire on those filming a protest in Bostan al Qaser in Aleppo.

According to Reporters Without Borders, at least 12 netizens and citizen journalists were killed between June 2014 and May 2015. IS executed two Syrian activists, Bashar Abul Azzem and Faysal Abulhalim, and accused them of spying in mid-2015. Bashar and Faysal were undercover reporters for the website and citizen group Raqqa Is Being Slaughtered Silently (also known as RSS), and they

75 Kaspersky Lab Global Research and Analysis Team, Syrian Malware, the evolving threat, August 2014, http://bit.ly/1pCJ0gK.
76 Interviews with released bloggers, names were hidden.
78 Interviews with two photographers who have taken refuge in Turkey, December 2011.
80 Interview with activist, January 2013, Aleppo, Skype.
81 Interview with lawyer from Aleppo, January 2013, Istanbul, Turkey.
were documenting IS’s crimes. Al-Moutaz Bellah Ibrahim of *Shaam News Network* was killed in Raqqa in May 2014.

International journalists, including those whose work is mainly featured online, also risk being targeted by Syrian militant groups, as three harrowing cases caught global media attention during the coverage period:

- In August 2014, James Foley, online journalist for the *Global Post*, was executed by IS.
- In August or September 2014, freelance journalist, Steven Sotloff, for *Foreign Policy, The Media Line* and *Time*, was beheaded by IS.
- In January 2015, a video surfaced showing the beheading Kenji Goto, a veteran Japanese reporter who founded the website *Independent Press* to cover humanitarian issues in 1996.

In one case from December 2013, IS militants killed 50 prisoners, including many journalists and media activists such as Syrian journalist Sultan al-Shami. Abdulwahab Mulla, a Syrian journalist known for his satirical YouTube comedy show “3-Star Revolution,” was kidnapped by masked gunmen on October 8, 2013. He was taken from his home in rebel-controlled areas of Aleppo. Many have hypothesized that extremist militants, such as IS, are behind the kidnappings. Many citizen journalists have lost their lives while documenting clashes. On May 21, 2013, 14-year-old citizen journalist Omar Qatifaan was killed while covering a battle between government forces and the Free Syrian Army near the city of Daraa in southern Syria, near the Jordanian border.

### Technical Attacks

After the growth of IS in the region, many anti-IS media outlets have come under different types of attacks.

- Al-Hal, a Syrian news website, claimed it came under a DDoS attack by pro-IS hackers in December 2014, bringing the website offline for 24 hours.
- In December 2014, the University of Toronto’s Citizen Lab released a report entitled, “Malware Attack Targeting Syrian ISIS Critics,” focusing on groups such as Raqqa is Being Slaughtered Silently (RSS), which documents IS human rights abuses committed by IS. Citizen Lab

---

91 Al-Hal, Facebook post showing DDoS attack, December 12, 2014, [http://on.fb.me/1EYVtpb](http://on.fb.me/1EYVtpb). The website is [https://7al.me](https://7al.me).
believes the malware was developed by IS or pro-IS hackers in order to discover more information about the nonviolent group.92

- Another media group, Souritna, was hacked by pro-IS hackers in January 2015. Its website was hacked due to Souritna’s statement of solidarity with the victims of the Charlie Hebdo attacks in Paris. The attackers were able to log into a File Transfer Protocol (FTP) service and delete the content of the website while uploading a new index page with the logo of IS.

At the same time, the Syrian Electronic Army (SEA) continues to target Syrian opposition websites and Facebook accounts, as well as Western or other news websites perceived as hostile to the regime. A huge shift in the level of hacking operations happened at the end of 2013, when the SEA was able to hack the New York Times website,93 the U.S. Marines website,94 Facebook,95 and many others. Most of the attacks occurred on the DNS level, which involved redirecting requests for the domain name to another server. The Twitter account of Barack Obama, run by staff from Organizing for Action (OFA), was briefly hacked by the SEA, resulting in the account posting shortened links to SEA sites.96 The hackers had gained access to the Gmail account of an OFA staffer. On March 17, 2013, the SEA hacked the website and Twitter feed of Human Rights Watch, redirecting visitors to the SEA homepage.97 These tactics continued with the high-profile hacking of Forbes in February 201498 and the Washington Post in May 2015.99

Though the hacktivist group’s precise relationship to the regime is unclear, evidence exists of government links or at least tacit support. These include the SEA registering its domain in May 2011 on servers maintained by the Assad-linked Syrian Computer Society;100 a June 2011 speech in which the president explicitly praised the SEA and its members;101 and positive coverage of the group’s actions in state-run media.102

Thailand

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Free</td>
<td>11</td>
<td>9</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>21</td>
<td>22</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>30</td>
<td>32</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>62</td>
<td>63</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 66.4 million
Internet Penetration 2014: 35 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2015 Status: Not Free

Key Developments: June 2014 – May 2015

- Military courts passed the longest sentences on record for insulting the monarchy online in 2015, including 56 years and 60 years in prison, reduced to 28 and 30 years on confession (see Prosecutions and Detentions for Online Activities).
- 400 people have been summoned and subjected to interrogation in various military compounds, often revealing their social media passwords as a condition of release (see Intimidation and Violence).
- “Digital economy” legislation drafted during the coverage period would erode user privacy and free speech rights online (see Regulatory Bodies and Legal Environment).
Thailand

Introduction

More Thai internet users were harassed and arrested during the coverage period than ever before in the wake of the 2014 coup. On May 20, 2014, General Prayuth Chan-ocha, commander of the Royal Thai Army, declared martial law. Two days later, as head of the military junta calling itself the National Council for Peace and Order (NCPO), the general cancelled the constitution, annulled the House of Representatives, and announced that the junta will rule the country for at least a year and five months before arranging a general election. The coup d’état was announced via all media, including Facebook and Twitter.¹

In the following weeks, the junta issued orders forbidding traditional media broadcasts, censored online news, and arrested or monitored hundreds of critics. Many of these measures were justified as part of a “returning happiness to Thai people” campaign, on grounds that controlling freedom of speech was necessary while the situation remained “abnormal.” Yet the junta’s plans, which include amending significant laws and passing a slew of new ones, will have a lasting impact.² It is attempting to pass a set of wide-ranging “digital economy” laws, including the country’s first cybersecurity and personal data laws. These draft laws came under heavy criticisms from academics and internet freedom activists, who argued that they would heavily impact privacy, curtail freedom of speech, and hamper the growth of the digital economy, contrary to its name.

Since the coup, academics and activists have been subject to overt surveillance, and more than 400 people have been summoned and subjected to interrogation in various military compounds throughout Thailand. Many were coerced to give up their login passwords to email and Facebook, so that authorities could monitor their communication.

The state already had ample means to infringe on users’ online freedoms in the form of computer-related crimes laws enacted after the 2006 coup, as well as criminal defamation charges, and oppressive lèse-majesté provisions in the penal code that punish criticism of the nation’s revered monarchy. Successive governments have blocked tens of thousands of individual websites and social media pages, and imprisoned several people for disseminating information and opinion online or via mobile phones under these laws. Anyone can lodge a lèse-majesté or defamation complaint based on any online content in Thailand, opening the door for various actors to use the charges against political opponents or to curb civic advocacy in the highly polarized political environment. Under the junta, these charges were heard by military tribunals, which have passed significantly longer sentences with no avenue for appeal. Punishments for insulting the monarchy online in 2015 exceeded 50 years in prison at least twice, though both the sentences were halved on the basis of subsequent confessions.

Obstacles to Access

Internet penetration has increased steadily in recent years, in part thanks to affordable government-run access programs, though usage remains concentrated in Bangkok and other urban centers, and speed and quality of service can vary. After the May 2014 coup, officials declared their intention to

establish a single gateway to the international internet, potentially enabling them to control or even shut down access nationwide.

Availability and Ease of Access

Internet penetration was at 29 percent in 2014, up from 26 percent in 2013; mobile penetration rose from 140 to 144 percent in the same period. Most Thai internet and smartphone users reside in the Bangkok greater metropolitan and southern regions, which boast a higher average household income. The lowest penetration is in the northeast, in part due to lack of service.

During the coverage period, the junta government approved the Provincial Electricity Authority’s THB 1,980 million program to extend electricity to remote areas. Under the “Return Happiness to the Thai People” program, the NCPO continued the ICT Free Wi-Fi program initiated under the previous government. This program, funded by the Broadcasting and Telecommunications Research and Development Fund for the Public Interest, offers wireless connections in various government and private buildings, which allow up to 15 users at a time to register with their national identification numbers for 20 minutes of free access per session, up to two hours per day. In 2014, this program had installed 120,000 access points countrywide in collaboration with select ISPs, and aims to install 130,000 more in 2015.

Partly as a result of efforts like this, official 2013 figures state 39 percent of Thai users accessed the internet free of charge, while another 23 percent paid less than THB 200 (US$6.73) a month. Connections reportedly function at speeds around 12 Mbps, most reliably in the greater Bangkok area.

Restrictions on Connectivity

The government has not historically blocked or throttled internet and mobile connections for political or security reasons. Within a week of the May 2014 coup d’etat, however, the Deputy Minister of Information and Communication Technology disclosed that he would propose a “national digital internet gateway” for internet service providers (ISPs) to use in connecting abroad. This initiative would be a cooperation between TOT and CAT Telecom, two state-owned telecom operators that have their own gateways, and six other ISPs. The deputy minister stated that this initiative would make it easier for the Ministry of Information and Communication Technology (MICT) to interrupt access directly. There were no further developments announced during the coverage period, though news reports in late 2015 said government agencies were exploring the legal foundation for

---

Thailand

a single gateway.

Thailand’s international bandwidth usage amounted to 1,563 Gbps in May 2015, and domestic bandwidth amounted to 2,323 Gbps, 195 percent and 132 percent higher than the previous year, respectively.  

ICT Market

The number of fixed-line internet users declined in 2014, while the number of mobile users continued to increase. As at the end of 2014, there were 97.10 million mobile numbers in Thailand, or an average of 1.4 numbers used per person. Thai people spend an average of THB 192 (US$ 5.6) per month on mobile expenses.

High-speed internet is still concentrated in a handful of large providers. According to statistics published in 2014, True Internet remained the market leader with a 37 percent market share, followed by TOT, a state-owned enterprise, with 31 percent, and 3BB at 29 percent. All other providers combined only amount to a 4 percent share of the market.

Regulatory Bodies

Since the May 22 coup d’état, there has been very little news on the progress of policies and plans that the MICT previously announced. This is not only because the junta government has centralized power, but also because the ministry itself is in the midst of a transition that is likely to lead to a power reshuffle. In December 2014 and January 2015, the Thai Cabinet approved draft laws establishing a Digital Ministry for Economy and Society and a Commission for Digital Economy and Society (CDES). On January 6, 2015, the Cabinet approved changing the ICT Ministry’s name to Digital Ministry for Economy and Society, and a restructuring of it in accordance with the subcommittees outlined in the draft digital promotion law: hard infrastructure, soft infrastructure, service infrastructure, digital society, knowledge resources, and digital economy promotion. Yet the process stalled amid disputes over the placement of the word “Digital” in the title, and the ministry’s status was unclear at the end of the coverage period.

The 11-member National Broadcasting and Telecommunication Commission (NBTC), an independent regulator viewed as broadly fair, still managed the industry as of May 2015, but its role was under threat. A simultaneous revision to the National Broadcasting and Telecommunication Commission law would transform NBTC from an independent regulator to a government agency under the jurisdiction of CDES. Surangkana Wayuparb, Director of Electronic Transactions Development Agency (ETDA) as head of digital law drafting team, said that the NBTC would remain independent under the revised law; however, the state will be in charge of policy. The CDES will be empowered to penalize noncompliant government or private entities, and will take over the allocation of spectrum for state

Thailand

and public interest uses, while the NBTC will only allocate spectrum for commercial use.\(^{16}\) Many analysts believe this would hinder Thailand's spectrum allocation.

The legislation was part of a “digital economy” strategy which the government said would promote the economy. At the end of the coverage period, a total of ten new laws or revisions are pending review by the Council of State before further submission to the junta-appointed National Legislative Council, all of which have raised concerns.\(^{17}\) Civil society and private sector actors called the laws obstructive, and criticized the focus on creating new agencies with broad powers. The draft laws would also transfer assets belonging to the Broadcasting and Telecommunications Research and Development Fund (BTRDF) under the existing NBTC law to a new “Fund for Developing Digital for Economy and Society” (FDDES). While the BTRDF is considered to operate in the public interest, the FDDES would be used to finance state or private “digital economy operators,” a potential conflict of interest.\(^{18}\) Furthermore, the draft laws also stipulate that representatives from state-owned TOT and CAT Telecom—which, as telecommunications providers, operate under licenses from the NBTC—would be appointed to the CDES. This would effectively give the regulated companies powers over the regulator, undermining the principle of free and fair competition.\(^{19}\)

In July 2014, the NCPO issued an order to delay a pending 4G spectrum auction for a year.\(^{20}\) Somkiat Tangkitvanich, Chairman of Thailand Development Research Institute, said that the delay may have been designed to allow the new laws to pass more control to the CDES.\(^{21}\) The auction is not expected to take place in 2015 because of a lack of preparation.\(^{22}\)

Limits on Content

Since the May 2014 coup, both the NCPO and the junta-appointed government have issued many orders and decrees that directly block online content that pertains to criticisms of the Thai monarchy, the NCPO, or the government. The form of censorship changed from obtaining a court order pursuant to Thailand's existing computer crimes law, to verbal requests for “cooperation.” Despite more pervasive censorship and pressure from the authorities, online space remains the easiest venue for dissidents and activists.

Blocking and Filtering

Although Thailand has long been heavily censoring websites, the censorship process became easier and faster after the coup. During the reporting period, the NCPO issued a number of decrees and orders governing content:


Thailand

- NCPO Announcement 18/2014 banned news reporting that disrupts national security, peace and order;
- NCPO Announcement 12/2014 asked social media users and operators to prevent content that incites violence or provokes protests, is illegal, or opposes NCPO rule.
- NCPO Announcement 17/2014 ordered ISPs to monitor for, and prevent dissemination of, any information that distorts facts, could provoke disorder, or affects national security;
- NCPO Announcement 26/2014 mandated surveillance and monitoring of social media by military agencies.23

In addition to these orders, the NBTC, in its role as regulator, requested that every ISP monitor and censor online content that may cause conflict and disrupt peace and order.24

Prior to the 2014 coup, the process to block websites was more rigorous, though it still lacked transparency. The competent officer at the Ministry of Information and Communication Technology (MICT) had to obtain court warrant after approval from the minister in order to block websites in accordance with Thailand’s computer crimes law. After the coup, public officials at any level, as well as ISP employees, were empowered to block websites directly, using their own judgement, under the auspices of the above-cited NCPO orders. As a result, there are no longer official censorship statistics.

Content that was most censored after the coup can be classified into two main categories: criticism of the Thai monarchy, and criticism of the NCPO or junta-appointed government. Blocked websites include foreign news websites such as Reuters and the UK-based Daily Mail newspaper; domestic news websites such as Prachatham; websites of human rights groups such as Human Rights Watch; academic websites such as Midnight University and Nitirat; personal websites of political bloggers and activists; and many Facebook and YouTube pages that contain anti-coup material.25

Content Removal

As with blocking, takedown requests were expedited and decentralized after the coup. The new process is highly unsystematic and uncoordinated to the point of seeming arbitrary. On February 6, 2015, the ISP CS Loxinfo called the webmaster of the Isra Institute’s Isra News Agency to request that the website take down a news article disclosing assets belonging to the brother of the leader of the junta. CS Loxinfo told the site that the article was perceived as instigating dissent. When the website operators contacted the MICT, however, the ministry could not verify the source of the request.26

The NCPO also harasses individuals to remove content from social media pages. Thanapol Eawsakul, the publisher of Fah Diaw Kan (“Same Sky Books”) magazine, was among many individuals

Thailand

briefly detained in mid-2014 and forced to sign an agreement not to publicly criticize the coup as a condition of release. In July 2014, Thanapol published opinions on various NCPO and government policies on his personal Facebook account. An army officer telephoned ordering him to remove the content on grounds that he was to post no political content that may create misunderstanding or a “bad attitude” toward the coup. Thanapol removed the posts, but documented the conversation on Facebook instead. In October 2014, the Fah Diaw Kan Facebook page described army officers disrupting a book fair event with political writers and academics. Once again, an army officer asked Thanapol to erase the post, claiming it made him feel uncomfortable.

Activists were also ordered to stop using Facebook for communication, including Krisdakorn Silalaksa, who was ordered by the army to cease his activities on Facebook in November 2014. He was a key advocate for the permanent opening of Pak Mun Dam sluice gates in Ubon Ratchathani province to allow fishing, a contentious issue between grassroots movements and successive Thai governments. The army also asked him to shut down his personal Facebook page because it contained “inappropriate” opinions.

Facebook removed content deemed to be lèse-majesté 30 times in the second half of 2014 based on requests from the Ministry of Foreign Affairs or the Thai CERT (Computer Security Incident Response Team). This represents a sharp rise from the five times requests with which it complied in the first half of 2014; it removed no content in late 2013.

Media, Diversity, and Content Manipulation

The slew of orders regulating content increased self-censorship and undermined the diversity of information available on the internet in Thailand. NCPO Announcement 14/2014 banned media interviews with any political actor who is not civil servant, yet the junta leader who appointed himself interim prime minister broadcast his own views nationwide on prime time TV several times a week.

Journalists trying to bypass the restrictions were censured. Wassana Nanuam, one of Thailand’s most famous military correspondents, described the daily routine of ousted Prime Minister Yingluck Shinawatra in narrative form in The Bangkok Post to avoid an interview format. She was reprimanded by the NCPO nevertheless, and apologized publicly. The article was removed from the Bangkok Post website.

Many media chose to self-censor in the oppressive atmosphere. Jaw Kw Tuen ("Shallow News"), a popular satirical internet TV program, temporarily suspended broadcasts after the coup until October 2014. Separately, Pinyo Trisuriyatham, a TV host, announced on June 9, 2014 that he decided to terminate the Amarin Newsnight program on one of the new digital TV channels, in order to

---

29 iLaw, “Before-after coup: self-censorship, online media censorship, community radio shutdowns, and other incidents”.
32 iLaw, “The report on online media suspension after the 22 May 2014 coup d’etat”.

776
There was no public documentation of paid actors manipulating political content on the internet during the coverage period, though officials encouraged citizens to monitor one another online (see, Surveillance, Privacy, and Anonymity), and many organized informally to harass the junta’s opponents (see Intimidation and Violence).

Digital Activism

Despite the dramatic uptick in persecutions and arrests since the coup, the online space remains a powerful outlet for individuals to communicate and organize political activities. In February 2015, the Foundation for Internet and Civic Culture, which is popularly known under its old name, the Thai Netizen Network, gathered over 20,000 signatures from people opposing the junta’s 10 digital laws, on grounds that they restrict freedom of speech and infringe upon privacy, and that the drafting process lacks public participation. Following the protest, the government’s drafting team stated that they would listen to public opinion. However, though the Council of State held one public hearing of one subsequent draft of these laws, the process remained as secretive as ever.

A number of outspoken activists and academics fled Thailand post-coup, but remain active on social media. Somsak Jeamteerasakul, a prominent historian and ex-professor at Thammasat University, relocated abroad and continues to publish his commentaries and political analysis via Facebook. Being physically outside the country allows these people to be more outspoken.

Violations of User Rights

An unprecedented number of internet users, bloggers, citizen journalists, and independent media were persecuted in 2014 and 2015. In addition to using existing laws such as the computer crimes law and lèse-majesté law harshly, the NCPO under martial law also issued numerous decrees and orders that severely infringe upon online rights. Moreover, the set of 10 draft digital laws that the Cabinet put forward in late 2014 and early 2015 is likely to have a long-term impact on the Thai online community if they are passed, granting the government vast surveillance and censorship powers.

Legal Environment

Article 45 of the Constitution of the Kingdom of Thailand 2007 guarantees broad freedom of speech, but was replaced with a 2014 interim constitution after the coup d’etat. Although it maintains the same safeguards, Thailand remains under martial law, which prohibits individuals and the media from any public political activity.

As in past years, the main legal apparatus used to charge internet users remains the charge of “infringing national security” under two laws, namely Clause 14 of the 2007 Computer related Crime Act (CCA) pertaining to content that affects national security, and Clause 112 of the criminal code pertaining to lèse-majesté. The CCA groups these online speech offenses with criminal activities like

---

Thailand

hacking or posting obscene material. The NCPO separately issued many decrees and orders that di-
rectly curtail freedom of speech.

The enforcement of existing laws and NCPO orders became more severe after NCPO Announcement
37/2014 on May 25, 2014, which stated that civilians conducting political activity would be court
martialed. The military court that tries these cases is a one-step court with no appellate or higher
division. In cases involving internet users that have already been tried, the military court has hand-
ed down more severe punishments. In lèse-majesté cases judged between 2010 and 2014 (during
which period the number of cases brought to trial showed a marked increase), the regular courts
handed down average jail terms of 4.4 years out of a possible 3 to 15 years. From the 2014 coup on-
ward, sentences issued by martial courts averaged 10 years imprisonment, reduced to 5 years after
confession.\(^\text{35}\)

The NCPO is pushing a “digital economy” policy through a set of 10 draft laws. The package would
revise the e-commerce law, the computer related crimes law, the National Broadcasting and Tele-
communication Commission law, and the Electronic Transactions Development Agency law, and
would create new laws for cybersecurity, personal data protection law, digital economy promotion,
the Fund for Developing Digital for Economy and Society, the Commission for Digital Economy and
Society, and the Ministry for Digital Economy and Society.\(^\text{36}\)

The appointment of a new commission, the Commission for Digital Economy and Society (CDES), is
central to the policy, and would assume responsibility for every facet of digital and technology regu-
lation. Sittichai Pokai-udom, advisor to the deputy prime minister, justified granting the commission
vast power, describing it as an attempt to improve on past, failed attempts to implement an e-gov-
ernment strategy. Yet the policy seemed geared toward consolidating control online. The draft CDES
law stipulates that CDES would have authority over every other ministry and government agency,
including the power to initiate disciplinary action to any government official or citizen who does not
comply with their orders.\(^\text{37}\) The laws would also grant authorities lawful interception powers without
a warrant and based on a perceived “threat,” which is not properly defined in the draft cybersecurity
law.

The revised criminal procedural law—which is not included in the digital economy package, but is
also pending before the National Legislative Council—separately grants surveillance powers to a
police official on the authorization of a superior and a court. The draft stipulates a wide range of
offenses for which surveillance powers are lawful: in addition to violations of national security and
organized crime, it includes very broad categories like “complex” crimes.\(^\text{38}\)

Under a separate draft law on the “prevention and suppression of materials that incite dangerous
behavior,” officials would require a warrant to access any private information that is deemed to
provoke sexually deviant acts, child molestation, child suicide, child torture, mass suicide, drug use,
terrorism, larceny, murder, or tortuous acts. Under this law, the creator and distributor of said infor-
mation faces one to seven years imprisonment and a fine of THB 700,000 (US$19,690) maximum; in

\(^{35}\) iLaw, “2014 Situation Summary Report 2/S: Lèse Majesté Cases: One Step Forward, Three Steps Backward,” Freedom of


\(^{38}\) iLaw, “draft criminal procedural law amendment: add wiretap authority, anyone exercising Miranda right is to be speculated guilty,” [in Thai], January 17, 2015, [http://law.or.th/node/3400](http://law.or.th/node/3400).
addition, any “access provider” (as defined by the existing computer related crime law) that knows such information exists in the computer system under their control but does not remove it also faces a maximum five year jail term and THB 500,000 maximum fine.39

Besides the problematic content of these laws, critics called the lawmaking process, which lacked participation from relevant stakeholders or public hearings, rushed and secretive. The Electronic Transactions Development Agency director who heads the legal drafting team said the top-down drafting process resulted from the urgency of the policy for the interim government.40 But they also harassed internet users and civil society groups who expressed alarm about the laws. On February 1, 2015, when students hosted a seminar on rights and freedoms under the pending laws, a military officer threatened the organizers for not requesting prior permission for the event and inserted himself, uninvited, as one of the panelists.41 Later that month, in the wake of online protests, authorities conceded they may remove some clauses of concern, combine some laws into new ones, and host closed-door hearings before submitting revised laws to the National Legislative Council for a vote; however, the process remained opaque.42

**Prosecutions and Detentions for Online Activities**

After the coup, the NCPO summoned hundreds of people to report for questioning in order to suppress potential dissent, and formally arrested people who mobilized public protests. Most of the people who were arrested were detained for seven days, the maximum duration allowed under martial law. Sombat Boonngam-anong, an anti-coup activist prominent since 2006, was one of those summoned to the NCPO right after coup. However, he refused to answer the summons on the grounds that the NCPO’s power was illegitimate and continued posting anti-coup statements on Facebook and Twitter. In June 2014, Thailand’s national security agency traced the IP address linked to the posts to his residence. Sombat was charged with three separate charges: not answering the NCPO summons, instigating dissent, and bringing computer information that affects national security into the system.43 Sombat was released on bail, but his cases are pending court-martial.44

The authorities targeted independent news outlets that operate online from undisclosed locations to avoid reprisals. Nut Rungwong (pseudonym), editor of the Thai E-News blog and news aggregator that has operated since the 2006 coup, was arrested for disseminating an article containing lèse-majesté content, although it was written by another writer based overseas.45 He was court-martialed and sentenced to nine years in jail in November 2014. The military court reduced the penalty

---

43  “Bringing false computer information into the system” is a cybercrime which has been repeatedly misapplied to content in libel prosecutions.
Thailand

to four years and six months in prison after he confessed. In June 2014, Katawut (pseudonym), an online radio operator, was charged with broadcasting lése-majesté content. A military court sentenced him to 10 years in jail behind closed doors, reduced to 5 years because he confessed. In a separate case, Banpot (pseudonym), another online radio operator, was charged with using online media to instigate hatred and publish lése-majesté content. In January 2015, the army arrested at least six people allegedly associated with Banpot, all of whom were charged with lése-majesté. The defendants were detained, all of their electronic equipment was confiscated, and all were forced to divulge their personal Facebook username and password. All six were accused of using Facebook or YouTube to distribute lése-majesté speech, photos, and video clips. The Thai public does not know the identity of the individuals behind Thai E-News, Banpot, or Katawut, but all of them have a significant fan base.

In addition to the media and citizen journalists, the NCPO also took numerous actions against political speech by regular internet users:

- Akaradej, a university student, was arrested over his Facebook posts in June 2014 and charged with lése-majesté. The court sentenced him to five years in jail, reduced to two years and six months after confession.

- Internet user Chaliew was accused of uploading Banpot radio clips to the website 4Shared. The content of this audio clip was deemed lése-majesté. He was summoned by the NCPO in June 2014 and has since been detained. He confessed to the crime. In August 2015, the Criminal Court sentenced him to a three year jail term, suspended for two years.

- Sirapob, accused of being the writer and poet behind the pseudonym “Roongsila,” was charged with posting three pieces of poetry deemed lése-majesté on the website Prachatai. Five army officers arrested him while he was travelling in July 2014. His case is currently being tried in secret by the military court.

- Thanes (pseudonym) was accused of sending an email linking to lése-majesté content in 2010. He has been in custody since July 2014. His case is being tried in secret by the Criminal Court.

- Charuwan, a factory worker in Ratchaburi province, was accused of posting lése-majesté content on Facebook. She denied posting the content to her account, saying she was framed, but was detained by the military from November 2014 to February 2015.

- Piya (pseudonym) was accused of owning a Facebook account, which he denied. In December 2014, the authorities charged him for publishing lése-majesté content on the account. The case is pending court decision.

47 Khatawut, Law (Military Court 2014).
Thailand

Sentences reached record lengths in August 2015, after the coverage period of this report. The 29-year-old Sasivimol was jailed for 56 years, reduced to 28 on confession, for seven Facebook posts considered lèse-majesté; separately, Pongsak Sriboonpeng was jailed for 60 years, reduced to 30 years on confession, for Facebook posts considered insulting to the monarchy.

In addition to arresting multiple Facebook users, police used Facebook Messenger as a kind of “bait” to trick Facebook users to reveal their sentiments toward the monarchy. For example, a user named Pongsak (pseudonym) was invited to discuss matters over the monarchy on Facebook Messenger. He was invited to travel to another province, where he was arrested upon arrival.

Later, police arrested Chayo (pseudonym) on the same charge, after Pongsak’s conversation log revealed that Chayo sent him statements and photos that are deemed lèse-majesté via Facebook Messenger.

Cultural content was also subject to increased scrutiny. This is reflected in the recent court decision on the case of a satirical play, titled “Wolf’s Bride,” staged at Thammasat University in October 2013. Two activists who starred in this play were later prosecuted and the court ruled them guilty of lèse-majesté. They both received two years and six months in prison. Typically the court would suspend sentences involving defendants who have never committed a crime, but the court refused in this case, ruling that this play was disseminated on the internet, which was deemed “egregious conduct.”

Chakrawut, a musician, was accused of operating three Facebook accounts which posted nine incidents of lèse-majesté content between 2011 and 2014. He was summoned by the NCPO in July 2014 and tried at the Ubon Ratchathani Criminal Court. In July 2014, he was sentenced to 30 years in jail, reduced to 15 years after confession.

Like any online environment, the Thai internet is fraught with misinformation, disinformation, fake news, and rumors, which are typically exposed and corrected by other internet users. Such content regarding the monarchy became cause for persecution after the coup. In February 2015, a fake Bureau of the Royal Household announcement pertaining to the king’s health was posted and widely circulated online. The police arrested a user they claimed to be the original poster, as well as the editor of ASTV, a mainstream media news website that posted the announcement and attendant article.

Besides lèse-majesté and political speech, libel is a longstanding problem in Thailand. Clause 14(1) of the current computer crimes law criminalizes “bringing false computer information into the system.” Although false computer information and libel are completely different in the legal terminology, suing people under both laws concurrently has become the norm. Attorney generals and judges have shown no understanding of the differences between the two laws, nor the fact that “false computer information” in the cybercrime parlance means technical crimes such as hacking, not the

---

Thailand

veracity of online speech. The vast majority of plaintiffs in these cases are government officials.

Examples of using computer crimes law to sue for libel in 2014 and 2015 include:

- The Ministry of Energy sued M.L. Kornkasiwat Kasemsri, an independent energy academic, for posting on his Facebook account that some diesel oil from Thailand is transported to Laos and sold at a lower price. The case is still pending trial.61

- The Royal Thai Navy sued the Phuketwan website for re-publishing a Pulitzer prize-winning Reuters article accusing Navy officials of profiting from a smuggling ring bringing Rohingya refugees from Myanmar. The Navy refused interviews to Phuket-based media and prohibits Phuketwan reporters from entering Navy bases. The case was pending at the end of the coverage period. 62

- Natural Fruit, a canned fruit company, sued migrant labor rights activist Andy Hall over dissemination of research reports that allege violations of labor rights in the company’s plants. The company is suing him in three separate cases, one of which uses the computer crimes law because the report was disseminated in online media. The case is still pending trial.63

During the same period, a number of computer crimes charges against journalists or public persons for libel ended in the plaintiff’s decision to drop the lawsuit or in dismissal by the court, suggesting they lacked merit, but were filed to intimidate the defendant. In one example from August 2014, the Secretary General of the Office of the Administrative Courts sued the Thai Press Development Foundation and Isra Institute, which published a news article about a memo from the secretary general to the police commissioner in support of an officer’s transfer. In November 2014, the Criminal Court dismissed the case on grounds that the plaintiff is a public person who must bear public scrutiny, and the defendant voiced opinion in good faith.64 In a separate September 2014 case, TV Channel 3 sued Supinya Klangnarong, an NBTC Commissioner, over comments she made in interviews and tweets about internal conflict over the channel’s transition to the digital system. In December 2014, Channel 3 withdrew the case. 65

Surveillance, Privacy, and Anonymity

In several cases where individuals were summoned or arrested, the authorities confiscated smartphones to peruse personal information and photos, or check for potential links to other people, before freeing the accused.

The NCPO has announced a clear policy regarding surveillance of internet users. A number of NCPO decrees and orders specifically mandate surveillance of online media. On June 23, 2014, Somyot Poompanmuang, deputy commissioner of the Royal Thai Police, publicly invited Thai people to “serve as eyes and ears” of the state. He encouraged everyone to take photos of people who display anti-coup symbols in public and online spaces, and submit those photos to the police. A monetary reward of THB 500 (US$14) per photo will be paid if the police can arrest and prosecute the photo

subjects. He also urged the public to inform the police via the *Jah Hook* ("Owl Sergeant") Facebook page.\textsuperscript{66} The MICT frequently said in interviews that the Thai government is monitoring private communication, such as the Line chat application.\textsuperscript{67} The same authority also said on more than one occasion that it would send officials to offices of popular social media platforms such as Facebook, Google, and Line, to seek their cooperation on suspending some specific individuals' accounts. There is no confirmation to date whether or not these companies agreed,\textsuperscript{68} after the planned meeting between NCPO, Google, and Facebook in Singapore was called off in May 2014.\textsuperscript{69} NCPO Announcement 26/2014 mandated surveillance and monitoring of social media by military agencies.\textsuperscript{70}

In September 2014, news reports said the MICT has ordered all ISPs to set up surveillance equipment at their data centers, implemented in an experimental phase from September 15.\textsuperscript{71} Some users speculate that the equipment could facilitate man-in-the-middle attacks for use with popular platforms Google and Yahoo, by setting up fake, unprotected sites which prompt users to enter their username and password before they reach the layer of encryption that protects the genuine login pages.\textsuperscript{72}

In February 2015, the Cabinet issued a resolution demanding that all users of pre-paid mobile phone cards and free Wi-Fi nationwide must be registered by July 31, 2015.\textsuperscript{73}

The Cyber Scout program, which began in 2011, continues unabated. The program, executed jointly by the ICT and education ministries, trains students to monitor and report online behavior they deem a danger to national security. There are currently over 120,000 cyber scouts nationwide, spanning 88 schools. The curriculum stresses recruiting new members and training cyber scout leaders.\textsuperscript{74}

**Intimidation and Violence**

Circumstances surrounding the NCPO summonses indicated that even those who cooperated were subject to pressure. Individuals were required to sign a written agreement promising not to voice political opinion or criticize the NCPO. A number of people were asked their Facebook passwords through a process of psychological harassment and were told by military officers that their personal


online conversations would be periodically monitored. In some cases, the military asked activists to post a statement on their Facebook account. This dictated statement essentially says that they have been treated with due respect by the military, police, and government officers, and that they will cease all forms of political movements to cooperate with the government in developing the country and supporting reform efforts.

Although the junta often claims that the coup was intended to fix deep-rooted problems in society and “return happiness” to the people, many new cases of intimidation arose in the social and political environment they established. Most were based on alleged violations of national security or lèse-majesté, which prompted persecution from fellow internet users as well as the state. Royalist groups organized online to report their opponents and file criminal charges against them. “National Trash Collecting Coalition,” a group of self-proclaimed vigilantes, has sued many internet users over lèse-majesté, including Surachai Sae-dan, an activist they accused in January 2015 of hosting an online radio show with lèse-majesté content. Tanat Tanawatcharanon, a former actor known as Tom Dundee, was sued for lèse-majesté by the “Network of Thai Subjects Who Volunteer to Protect the Monarchy in Facebook” over political speech he made on the red-shirt stage in November 2013, which someone taped and distributed on YouTube in June 2014. He was arrested in June 2014.

Facebook’s “report” feature, which allows users to flag content which violates the site’s terms, was used as a tool for harassment and intimidation. After rumors surfaced that Tang Acheewa (pseudonym), a red-shirt activist, was granted political asylum in New Zealand, the Facebook page of United Nations High Commissioner for Refugees (UNHCR) was bombarded with condemnation until the office temporarily suspended the page.

Technical Attacks

There have been sporadic reports of hacking attacks on online news outlets in Thailand in the past. None were documented during the coverage period of this report, though hackers did target government sites.

Tunisia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>39</td>
<td>38</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population:</td>
<td></td>
<td>11 million</td>
</tr>
<tr>
<td>Internet Penetration 2014:</td>
<td></td>
<td>46 percent</td>
</tr>
<tr>
<td>Social Media/ICT Apps Blocked:</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Political/Social Content Blocked:</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Bloggers/ICT Users Arrested:</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Press Freedom 2015 Status:</td>
<td>Partly Free</td>
<td></td>
</tr>
</tbody>
</table>

Key Developments: June 2014 – May 2015

- In September 2014, Tunisia’s first privately owned submarine fiber-optic cable was inaugurated, thus easing the state’s monopoly on the country’s connection to the international internet (see Restrictions on Connectivity).

- Tunisia’s telecoms regulator, the INT, took steps towards greater transparency and accountability through the introduction of new regulations surrounding the licensing of ISPs (see Regulatory Bodies).

- A surge of terrorist attacks has led to calls to block or remove extremist content online. Authorities from the ICT ministry have maintained that the country will not resort to blocking, although the ministry has sought greater cooperation with social media companies to take down content that incites violence or extremism (see Blocking and Filtering and Content Removal).

- A handful of Tunisians were prosecuted for their online activities. Rached Khiari, director of the Al Sada News website, received a three-month suspended sentence for defamation after publishing a video in which a third party insulted a judge (see Prosecutions and Detentions).

- After being sentenced in absentia to three years in prison by a military court, blogger Yassine Ayari was arrested upon returning to the country. In a retrial and subsequent appeal, Ayari’s sentence was ultimately reduced to six months and he was released in April 2015. Ayari was found guilty of defaming the military for Facebook posts in which he criticized the minister of defense (see Prosecutions and Detentions).

- Amid heated presidential elections, the website of the Independent Electoral Commission was attacked, temporarily suspending voter registration (see Technical Attacks).
Tunisia

Introduction

The internet remains partly free in Tunisia. Although the state-controlled Tunisie Télécom (sometimes referred to as TT) maintains a monopoly over the country’s domestic internet backbone, two ISPs inaugurated Tunisia’s first privately operated fiber optic submarine cable. Tunisia’s telecoms regulator, the INT, introduced new licensing regulations and continues to make strides towards ensuring greater transparency and accountability.

As the government grapples with increased terrorist attacks, authorities have resisted calls to reinstitute blocking and filtering. Instead, officials have declared their intention to work together with social media companies to remove content that incites extremism or violence. Digital rights activists have expressed fears over surveillance now that the Technical Telecommunications Agency (ATT) is up and running, despite no clear mandate and oversight mechanisms.

Furthermore, Tunisia’s fragile internet freedom remains threatened by a number of laws dating from the Ben Ali era, including the Telecommunications Decree and the Internet Regulations. The judiciary continues to restrict free speech through the prosecution of users over content posted online, mainly regarding defamation, religion, and insults to state bodies. Blogger Yassine Ayari was tried by a military court and served prison time over charges related to the defamation of the military. The editor of Al Sada News received a three-month suspended sentence for defamation regarding a video published to the website in which a third party insulted a judge. Several other Tunisians were detained or suffered legal harassment on vague charges.

The internet was first launched for public use in Tunisia in 1996, and the first broadband connections were made available by the end of 2003. The online landscape changed dramatically with the ouster of autocratic president Zine El Abidine Ben Ali on January 14, 2011. His repressive censorship apparatus largely dissipated and internet users have started to enjoy an unprecedented level of open access. After the passage of a new constitution last year, Nidaa Tounes emerged as the country’s largest political party in the October 2014 parliamentary elections. The first round of presidential elections followed in November, with a run-off held one month later. Béji Caid Essebsi defeated incumbent Moncef Marzouki in a tightly disputed contest that spilled over into the online media landscape.

Obstacles to Access

_Growth in mobile internet subscriptions has underpinned an increase in internet penetration in Tunisia over the past year. Private operators Ooredoo Tunisie and Orange Tunisie inaugurated their own international submarine cable, boosting bandwidth capacity. However, the telecommunications market remains centralized in the hands of three major players, with state-controlled Tunisie Télécom continuing its monopolistic control over the internet backbone. Tunisia’s telecoms regulator has also taken steps towards greater transparency and accountability through the introduction of new licensing regulations._

Availability and Ease of Access

According to the International Telecommunication Union (ITU), internet penetration stood at 46
Tunisia

percent in 2014, up from 34 percent in 2009. The number of fixed broadband subscriptions per 100 inhabitants dropped from 4.86 to 4.44 over the past year, due to a preference for mobile broadband subscriptions. As of March 2015 there were more than 4.5 million subscriptions to 3G mobile data plans compared to some 500,000 fixed broadband subscriptions. Internet connections through 3G USB keys exceeded 1.1 million subscriptions.

The number of computers per 100 inhabitants rose from approximately 12 in 2009 to nearly 22 as of March 2015, while the number of internet subscriptions (fixed and 3G USB keys) is estimated to have exceeded 1.7 million as of March 2015. The popularity of mobile phones is also on the rise, with over 14 million mobile phone subscriptions and a penetration rate of 127.6 percent as of April 2015.

Nonetheless, internet access remains beyond the reach of a large segment of the population. According to a World Bank report released in January 2014, “the poorest 40 percent of the population would need to spend over 40 percent of their income to afford high speed internet.” USB keys used for 3G internet cost at least TND 40 (approximately US$20.5), while the service costs TND 25 (US$13) per month for 10GB of data.

Thus, many Tunisians access the internet at their workplace or at privately owned cybercafes known as “publinets,” where one hour of connection costs at least 1 TND (US$ 0.51). Before 2011, wireless access in cafes and restaurants was not permitted by law, which allowed only licensed ISPs to offer access. Nonetheless, since the revolution it has become common for cafes and restaurants in major cities to offer free internet access without any registration requirements, attracting mainly young social network users. The ICT ministry issued new regulations on the provision of internet access by cybercafes on July 29, 2013.

Fixed-line internet subscribers must first buy a landline package from Tunisie Télécom (TT), which manages the country’s 130 Gbps bandwidth capacity, before choosing one of 11 ISPs. The TT landline package costs 45 TND (US$23) for per three-month subscription period. ISP prices range from TND 10 (US$5) a month for a connection speed of 1 Mbps to TND 50 (US$25) for a connection speed of 20 Mbps. Although there are no legal limits on the data capacity that ISPs can supply, the bandwidth remains very low and connectivity is highly dependent on physical proximity to the existing infrastructure.

---

Tunisia

Restrictions on Connectivity

The Tunisian government does not impose any restrictions on ICT connectivity. However, Tunisie Télécom remains the sole manager of the country’s 10,000KM fiber-optic internet backbone covering the entire territory. Tunisie Télécom also acts as a reseller to domestic ISPs, granting it an oversized role in the country’s internet governance. However, some positive signs have emerged of late. In September 2014, private operators Ooredoo Tunisie and Orange Tunisie inaugurated their own international submarine cable, thus easing the monopoly of Tunisie Télécom on Tunisia’s international submarine communications cables. The 175km long cable which links Tunisia to Italy is the first privately owned cable to enter into service in Tunisia.

ICT Market

The main providers of internet service are Tunisie Télécom, Ooredoo Tunisie, and Orange Tunisie. The state controls a 65 percent stake in Tunisie Télécom, while the remainder is owned by Emirates International Telecommunications (ETI). In June 2013, ETI announced its plan to sell its Tunisie Télécom shares, citing employees’ strikes over higher salaries as a reason for the move. Ooredoo Tunisie is a subsidiary of the multinational company Ooredoo, which is partially owned by the state of Qatar. Finally, Orange Tunisie has been controlled by the state since 2011, when a 51 percent stake was seized from Marwan Ben Mabrouk, son-in-law of fallen dictator Ben Ali. The remaining 49 percent stake is owned by the multinational group Orange.

Regulatory Bodies

The Ministry of Communication Technologies and Digital Economy (ICT ministry) is the main government body responsible for the ICT sector. The National Instance of Telecommunication (INT) is the regulator for all telecom and internet-related activities and has the responsibility of resolving technical issues and disputes between actors.

The INT’s governance body is made up of mainly government officials nominated by the ICT Minister, which activists argue leads to a lack of regulatory independence. Nevertheless, the INT has initiated some positive changes in internet policy, namely through the introduction of a more liberal domain name chart and an invitation to independent arbitrators from civil society to help develop a new Alternative Domain Name Dispute Resolution Process.

Internet policy is decided by the INT and executed by the Tunisian Internet Agency (ATI), a state body governed by a board of trustees comprised of representatives from the main shareholder, Tunisie Télécom. The company controls 37 percent of ATI shares and the state owns a further 18 percent, while the remaining 45 percent is divided among private banks. The head of the ATI is appointed by the ICT ministry. The INT and ATI manage the “.tn” country domain. Under Ben Ali, the ATI was a government organ for surveillance and censorship. The ATI now manages the internet exchange point (IXP) between national ISPs that buy connectivity from Tunisie Télécom, as well as the allocation of internet protocol (IP) addresses. The agency also provides direct internet access to public institutions.

---

Tunisia

In December 2014, the government of then-prime minister Mehdi Jomaa passed decree n°2014-4773 which regulates the granting of business licenses to ISPs, replacing the Telecommunication Decree of 1997. Under the new decree, ISPs are subject to prior authorization from the ICT ministry, after consulting with the ministry of interior and the INT. Article 8 established a new advisory board tasked with examining licensing requests and advising on matters related to infractions and sanctions. The board is presided over by the ICT minister or his representative and is composed of representatives from the ministries of defense, interior, ICT, and commerce; the INT; and the Union for Industry and Commerce (UTICA). Businesses wishing to apply for a license need to have a standing capital of at least TND 1 million (approximately US$20,000). Licensing applications must be answered by the ministry within one month.

Limits on Content

As the authorities grapple with mounting terrorist attacks, attention has turned to the fight against online extremism. Government agencies have alluded to plans to block or remove extremist content online, although little action has been taken for now. Blocking and filtering have ceased since the toppling of the Ben Ali regime four years ago. Tunisian users continue to enjoy an open internet in the country. However, in the absence of legal reforms, laws regarding censorship and intermediary liability for the Ben Ali era continue to pose a threat to users. Many remain hesitant to cross red lines on sensitive topics over fears of arrest and prosecution under harsh defamation laws.

Blocking and Filtering

Censorship remains sparse in Tunisia, with no instances of politically motivated blocking over the past year. Popular social media tools such as Facebook, YouTube, Twitter, and international blog-hosting services are freely available.

In September 2014, the country’s telecommunications industry regulator and the ICT ministry denied media reports alleging that the three operators would soon be blocking Voice over Internet Protocol (VoIP) services like Skype and Viber for 3G users except under special pre-paid packages. In a statement published on September 16, the ministry said that such a move would violate the principle of network neutrality guaranteed under Article 26 of the Telecommunications Law.

Following several attacks by Islamist extremists, government officials have called for the filtering of web pages affiliated with terrorism. Speaking after an attack that left 15 soldiers dead on July 16, 2014, then-interior minister Lotfi Ben Jeddou reiterated his calls for the monitoring and the filtering of the internet, which he says “remains outside the control of the State.” There were no indications...

---

13 [the ministry’s clarifications regarding alleged reports on plans by public telecommunication network operators to suspend Skype and Viber services] Babnet Tunisie, September 16, 2014, http://www.babnet.net/rttdetail-91636.asp
Tunisia

the authorities proceeded with these calls, however. Telecommunications Minister Noomane Fehri has stated he “will not adopt a policy of blocking websites whatever their danger to us because we believe this solution is technologically useless.”

Content Removal

While authorities admit filtering “won’t solve the problem” of users accessing extremist content, the telecommunications ministry has revealed it is coordinating with social media companies to suspend pages that incite violence or extremism.

According to Article 9 of the 1997 Internet Regulations, ISPs are required to continuously monitor content to prevent the dissemination of information “contrary to public order and good morals.” Laws such as these that impose legal liability on intermediaries have been used to take down political or social content in violation of free speech protections. For instance, in March 2015, the satire news site tounesnews.com was shut down for a few days by the web hosting service OVH following a removal request from the Tunisian authorities for spreading false news. It was reported that the site was targeted over a satirical article accusing Wided Bouchamaoui, head of the industry and commerce union, of tax evasion.

Media, Diversity, and Content Manipulation

Tunisia’s online media landscape is vibrant and open. Since the revolution, numerous online sources of information have been launched alongside new newspapers, radio stations, and television channels, enriching the information landscape through the addition of viewpoints from a diverse range of social actors. In June 2014, a group of journalists and web developers launched Inkyfada.com, a ‘slow journalism’ web magazine. The publication makes use of mapping and data visualization tools to help readers understand complex stories.

Nonetheless, Tunisia’s post-revolutionary vibrancy has not eliminated all self-censorship. Some online activists still avoid crossing red lines over fears of legal prosecution. Still, users are more open to discussing religion, the army, and other sensitive issues on the web compared to traditional media platforms.

The importance of online news sources has been recognized by politicians. In the country’s newfound democracy, partisan groups have used the internet to campaign. The information battle was particularly fierce during the second round of the presidential elections in late 2014, when the respective supporters of outgoing president Moncef Marzouki and current president Beji Caid Essebsi accused each other of spreading rumors. Nevertheless, the unprecedented openness of the Tunisian online sphere in the post-Ben Ali era has greatly diluted the influence of such content.

18 Nejma Rondelez, “Inkyfada.com, le magazine web tunisien qui prend le temps” [Inkyfada.com, the Tunisian web magazine that takes its time] Al Huffington Post, July 15, 2014, http://huff.to/1QeiuFf
Tunisia

Candidates also made positive use of social networking sites to reach out to voters and answer their questions.21

Digital Activism

Tunisian youth and civil society organizations have continued to use digital media for initiatives relating to political and social issues. Over the past year, a number of organizations used new technology to monitor the electoral process. The nongovernmental organization (NGO) Cahiers de La Liberté launched “Birrasmi” (“Really?”), a platform to fact-check the veracity of statements made by candidates in the country’s legislative and the presidential elections.22 The election monitoring group Mourakiboun created a quick vote-counting platform to aid in election observation.23 Relying on data provided by its observers, the group visualized figures related to the elections such as turnout rates and results.24

In July 2014, the transparency NGO al-Bawsala launched “Marsad Baladia,”25 a project that collects and publishes data related to local municipalities.26 Published data includes the budget and resources allocated to each municipality, as well as information on the progress of various municipal projects. The data allows the NGO to rank municipalities according to their commitment to transparency.

Violations of User Rights

While Tunisia has taken significant steps to promote internet access and reverse online censorship, the country’s legal framework remains a significant threat to internet freedom. Despite the adoption of a new constitution hailed as “democratic,”27 the absence of legal reforms continues to hold Tunisia back. Most problematically, the judiciary continues to employ laws from the Ben Ali-era to prosecute users over online expression. Criminal defamation remains one of the biggest obstacles to independent reporting.28

While several users have been charged with insulting state bodies or religious values. At the same time, the creation of a new cybercrime investigative agency has led to fears that technology could once again be misused to perform unchecked government surveillance on Tunisian citizens in a return to Ben Ali-era practices.

Legal Environment

The 2014 constitution, the first to be passed since the 2011 revolution, enshrines the right to free expression and freedom of the press, and bans “prior censorship.” Specific articles guarantee the right to privacy and personal data protection, as well as the right to access information and commu-

24 Mourakiboun, Facebook post, December 22, 2014, http://on.fb.me/1Nfr4qB.
Tunisia

Despite improvements to the constitution, the repressive laws of the Ben Ali regime remain the greatest threat to internet freedom. Article 86 of the Telecommunications Code states that anyone found guilty of “using public communication networks to insult or disturb others” could spend up to two years in prison and may be liable to pay a fine. Articles 128 and 245 of the penal code also punish slander with two to five years’ imprisonment. Article 121 (3) calls for a maximum punishment of five years in jail for those convicted of publishing content “liable to cause harm to public order or public morals”. In addition, Tunisia’s code of military justice criminalizes any criticism of the military institution and its commanders.

Tunisia’s press code does not provide bloggers and citizen journalists with the same protections afforded traditional journalists. Article 7 defines a “professional journalist” as a person holding a BA degree who “seeks the collection and dissemination of news, views and ideas and transmits them to the public on a primary and regular basis,” and “works in an institution or institutions of daily or periodical news agencies, or audiovisual media and electronic media under the condition that it is the main source of income.”

Prosecutions and Detentions for Online Activities

Several users were arrested or prosecuted against international norms of free speech over the past year:

- In October 2014, the primary court of Tunis sentenced Rached Khiari, the director Al Sada News website, to a suspended jail term of three months over the publication of a video deemed defamatory. The public prosecutor filed the court complaint in which Khiari was accused of insulting others through public communication networks under Article 86 of the Telecommunication Code. Although he is the director of a news publication, Khiari was not prosecuted under the 2011 press code. In the video, published in March 2014, a mother cursed the judge who sentenced her son, a controversial Islamist activist, to jail. The mother received a three month prison sentence.

- In December 2014, Tunisian authorities arrested blogger Yassine Ayari as he returned to Tunis from a trip abroad, six weeks after he was convicted in absentia of defaming the military institution. Ayari was sentenced by a military court, under article 91 of the military justice code, to three years in jail. He was found guilty of “defaming army officers and se-

---

nior defense ministry officials” in a series of Facebook posts in which he criticized Minister of Defense Ghazi Jeribi for refusing to appoint a new head of military intelligence and for weakening military institutions. In a retrial held on January 20, Ayari’s verdict was reduced to a one-year sentence. Ayari appealed his conviction and on March 3 the military court of appeals reduced his jail term to six months. Ayari was released on April 17.

- On May 7, 2015, a primary court sentenced in absentia police union leader Walid Zarrouk to one year in jail for “insulting others through public communication networks” over a 2013 Facebook post. In the post, Zarrouk accused the then-general prosecutor of the Tunis Tribunal, Tarek Chkioua, and minister of justice Nourredine Bhiri of “ politicizing prosecutions.”

- On September 21, 2014, three members of the collective blog Nawaat were detained for filming without authorization on the premises of a court in Bizerte, in northern Tunisia. Sami Ben Gharbia, Henda Chennaoui, and Callum were at the court covering the trial of a comedian and were released the same day without charges.

- In early January 2015, the Cassation Court acquitted blogger Hakim Ghanmi of defamation charges for criticizing the staff of a military hospital in a blog post. The case dates back to May 2013 when Ghanmi stood trial before a military court in Sfax on charges of “undermining the reputation of the army,” “ defamation of a public official,” and “disturbing others through public communication networks.” Under the initial verdict, Ghanmi was cleared of two of the charges, but fined TND 240 (US$ 130) for defamation of the army.

- Jabeur Mejri continues to face legal harassment following a March 2014 presidential pardon that saw him avoiding over seven years of prison for publishing cartoons depicting the prophet Mohammed on his Facebook page. One month later, Mejri was sentenced to eight months in prison for “insulting a public servant” during an investigation into his alleged embezzlement of funds. He stood accused of stealing TND 1,600 (US$870) worth of train tickets while working for the Tunisian national railway company. He was eventually pardoned again and released on October 15, 2014.

---

41 In 2012, Mejri had been convicted along with his friend Ghazi Beji of “insulting others through public communication networks” under Article 86 of the Telecommunications Code, and publishing content deemed offensive to Islam and “liable to cause harm to public order or public morals” under Article 121 (3) of the Tunisian Penal Code. Beji, who fled the country and obtained political asylum in France in June 2013, was sentenced in absentia to seven and half years of prison for publishing an e-book satirizing Prophet Muhammad’s biography on Scribd.
42 “Tunisie: Grâce par la présidence, Jabeur Mejri a été libéré," [Tunisia: Pardoned by the presidency, Jabeur Mejri has been released] Al Huffington Post, October 15, 2014, http://huff.to/1jWJbS.
Tunisia

Less controversially, authorities have also arrested several individuals for advocating extremism or cyberattacks:

- On July 25, 2014 the Interior Ministry announced the arrest of a Facebook page administrator who “adopts and spreads Takfiri-Salafi-jihadist ideology” and confiscated his computer.\(^43\) In August of the same year, police arrested six more individuals for “celebrating the murder of Tunisian soldiers” and “incitement to terror acts” on social networking sites.\(^44\) Clear details about the cases were not available.

- On February 10, 2015 police arrested six members of the hacker group Fallaga for hacking national and foreign websites.\(^45\) As part of the #JesuispasCharlie cyberattack targeting French websites, the group hacked the website of the National Syndicate of Tunisian Journalists for issuing a statement in support of Charlie Hebdo. They also hacked the website of the ATI. The group stated that hacking the ATI website was not “politically motivated” but was rather aimed at highlighting the security vulnerabilities of government-run websites.\(^46\) Though the Interior Ministry had described them a takfiri group, accusing other Muslims as being apostates, Fallaga denied any support for terrorism.\(^47\) Three of the hackers have since been released, while three remained in detention as of mid-2015.

Surveillance, Privacy, and Anonymity

Surveillance remains a strong concern in Tunisia due to the country’s history of abuse under the Ben Ali regime. While there have not been any reports of extralegal government surveillance in the post-Ben Ali period, the deep-packet inspection (DPI) technology once employed to monitor the internet and intercept communications is still in place, sparking worries that the technology can be reactivated if desired.

The creation of a new government surveillance agency in November 2013 raised concerns among human rights and privacy groups, particularly given the lack of transparency surrounding its duties. The Technical Telecommunications Agency (ATT) was established by decree n°2013-4506 under the former administration of Ali Laarayedh. The decree tasks the ATT with “providing technical support to judicial investigations into information and communication crimes,” but neither defines nor specifies these crimes.\(^48\) Netizens immediately criticized the decision for its lack of parliamentary scrutiny, as well as a failure to provide the body with a clear and limited mandate, with independence from government interference, and with mechanisms to guarantee user rights.\(^49\) According to Article 5 of the decree, the ATT’s activities are not open to public scrutiny.

The ICT minister is charged with appointing the ATT’s general director and department directors. An oversight committee was established “to ensure the proper functioning of the national systems for


\(^{44}\) Tunisian Interior Ministry. Facebook post: a statement on the arrest of 6 “takfiris” over incitement to terror acts on social networking, August 12, 2014, http://on.fb.me/1XqSv2W.


Tunisia

controlling telecommunications traffic in the framework of the protection of personal data and civil liberties." The committee mainly consists of government representatives appointed from the ministries of ICT, human rights and transitional justice, interior, national defense, and justice.

Despite fierce criticism, the ATT started operating in “full capacity” in the summer of 2014 after the appointment of Jamel Zenkri, who previously served at the ATI and the INT, as general-director. Responsibilities for conducting internet surveillance for the purposes of law enforcement have thus been transferred to the ATT from the ATI, which often assisted the judiciary in investigating cybercrime cases despite the absence of a law requiring it to do so.

Fears over the ATT have been boosted by the fact that Tunisia’s transitional authorities have been slow to initiate any legal reforms that would protect citizens from mass surveillance. Draft amendments by Tunisia’s Data Protection Authority (INPDP) to amend the country’s 2004 privacy law have not been discussed by the constituent assembly or by the new parliament elected in October 2014.

Laws that limit online anonymity also remain a concern in the post-Ben Ali era. In particular, Articles 9 and 87 of the 2001 Telecommunication Code ban the use of encryption and provide a sanction of up to five years in prison for the unauthorized use of such techniques. While there have been no reports of these laws being enforced, their continuing existence underscores the precarious nature of Tunisia’s newfound and relatively open internet environment.

**Intimidation and Violence**

In addition to legal prosecution, users must also be wary of extralegal attempts to silence online activists. While in prison, Jabeur Mejri had reportedly received death threats. In a statement published on September 23, 2014, Mejri’s support committee reported that one prisoner shouted: “He is an atheist [referring to Mejri], and I will kill him just like we murdered Chokri Belaid,” a secular politician assassinated in 2013. In response to these threats, the prison’s administration transferred Mejri to another cell to ensure his safety.

Online threats are also present in the country. On January 5, 2015, liberal blogger Lina Ben Mhenni received death threats from a Twitter user under the handle “@ISItunisie.” The account has since been suspended. This was not the first time she has been harassed; threats led to Ben Mhenni being placed under police protection in August 2013.

---


55 Lina Ben Mhenni Facebook page, Facebook post; January 5, 2015, [http://on.fb.me/1fZub7E](http://on.fb.me/1fZub7E).

Tunisia

Technical Attacks

Since Ben Ali’s fall, there have been no reported incidents of cyberattacks perpetrated by the government to silence ICT users. However, other groups have employed these methods to intimidate activists and organizations with whom they disagree.

- On July 10, 2014, a cyberattack targeting the website of the independent electoral commission temporarily suspended voter registration via SMS and the online registration platform.57

- On November 17, 2014, the video page of Radio Mosaique FM was targeted by a cyberattack aiming to remove its videos. The attack was reportedly led by group of “revolutionary” hackers targeting sites linked to the Democratic Constitutional Rally (RCD), the former ruling party of Ben Ali.58

- On December 31, 2014, the group Fallaga launched cyberattacks targeting government websites such as those of the ministries of culture, transportation, and women to call for the release of blogger Yassine Ayari.59 One week earlier, the group also targeted the website of the election observer NGO Mourakiboun, accusing the group of turning a blind eye to “gross violations” during the elections.60

Key Developments: June 2014 – May 2015

- Law No. 5651 on Regulating the Internet was amended in September 2014, broadening the scope of administrative blocking and allowing the authorities to access user data without a warrant. While the Constitutional Court overturned these provisions a month later, they were once again passed in March 2015 following the retirement of the court’s chief judge. As a result, Turkey’s regulator may ban content to secure the protection of life and private property, protection of national security and public order, prevention of crimes, and protection of public health without a prior court order (see Blocking and Filtering).

- Twitter, Facebook, and YouTube were temporarily banned in April 2015 until they complied with requests to restrict access to sensitive content, including material related to the abduction and killing of a public prosecutor. In the first half of 2015, 92 percent of all court orders to remove content received by Twitter worldwide originated in Turkey (see Blocking and Filtering and Content Removal).

- Dozens of Turkish users faced charges for criticizing the government or public officials, particularly on Twitter. Recep Tayyip Erdoğan has filed criminal complaints against more than 67 people for allegedly insulting him online since he moved from the premiership to the presidency in August 2014 (see Prosecutions and Detentions).

- Following corruption scandals and leaks of the telephone conversations of top government officials, senior staff at Turkey’s telecommunications regulator were arrested for conducting illegal wiretaps. In a separate incident, leaked emails revealed that Turkey’s civilian police force had contracted with the Italian company Hacking Team to spy on Turkish citizens from 2011 to 2014. Meanwhile, the Homeland Security Act, passed in March 2015, increased the amount of time for which investigators may conduct wiretaps and other signals intelligence operations without a court order from 24 to 48 hours (see Surveillance, Privacy, and Anonymity).
Turkey

Introduction

Elections, protests, and scandals marked the online sphere in Turkey over the past year. As the political and social significance of social media has grown, so have legal restrictions on their use. Social media were reportedly listed as one of the main threats to national security in the National Security Council’s National Security Policy Document, and President Recep Tayyip Erdoğan was quoted as saying “I am increasingly against the internet every day” during a meeting with a press freedom delegation. Erdoğan won Turkey’s first direct presidential election in August 2014. That same month, former foreign minister Ahmet Davutoğlu replaced Erdoğan as prime minister and chairman of the ruling Justice and Development Party (AKP).

During the highly publicized “Occupy Gezi” protests in May and June 2013, the number of Turkish Twitter users rose from 2 to 8 million. The role of social media in weakening the ruling party’s control over the flow of information has led to new laws to censor content. Amendments to Law No. 5651 on Regulating the Internet were passed in February 2014, September 2014, and March 2015, broadening the scope of regulators’ powers to block content without a court order, increasing burdens on intermediaries, and eroding the privacy of users’ personal data. In total, some 80,000 websites were reportedly blocked in the country as of May 2015.

The Constitutional Court has served as a crucial check on executive authorities in the fight for internet freedom, ruling in early 2014 that the wholesale blocking of Twitter and YouTube was unconstitutional. Access to the platforms was eventually restored, but they were temporarily blocked again in April in order to force the companies to restrict access to certain content for Turkish users. Blocking orders tend to coincide with important political events, such as an election, intelligence leak, hostage crisis, or corruption scandal. The Constitutional Court also overturned some of the most problematic aspects of the amendments to Law No. 5651 that were passed in September 2014. However, the AKP reintroduced the provisions as part of an omnibus bill in January, and they were passed in March 2015, thereby expanding Law No. 5651 to allow for the blocking of content on matters concerning the protection of life and private property, protection of national security and public order, prevention of crimes, and protection of public health.

Dozens of Turkish users were detained and prosecuted for their online activities over the past year, often arbitrarily singled out for content that was satirical in nature. The most common charge was “insulting” public officials, namely President Erdoğan, who has filed criminal complaints against more
Turkey

than 67 people for their online activities since he was elected in August 2014. While most receive suspended sentences that will not place them in jail unless they reoffend, the aggressive prosecutions have had a significant chilling effect on ordinary social media users and well-known activists alike. The abuse of government surveillance, the bulk retention of user data, and measures to undermine encryption and anonymity also remain serious concerns, particularly after the passage of the Homeland Security Act in March 2015 and the leak of documents showing the use of malware tools by a Turkish civilian police force. Overall, internet freedom is highly imperiled in Turkey.

Obstacles to Access

Penetration rates have continued to increase over the last few years, but obstacles to internet access in Turkey remain. Investment is still needed to improve the infrastructure. The regulatory agency responsible for information and communication technologies (ICTs) is well staffed and has a dedicated budget. However, the fact that its board members are government appointees is a potential threat to its independence, and its decision-making process is not transparent.

Availability and Ease of Access

Penetration rates have continued to increase over the last few years, but obstacles to internet access in Turkey remain. According to the International Telecommunication Union, internet penetration stood at 51 percent at the end of 2014, up from 36 percent in 2009. The number of internet subscribers in Turkey increased by 7.6 percent in the third quarter of 2014 as compared with the second quarter, according to Turkey’s Information and Communications Authority (BTK), the regulator responsible for ICTs. Turkey ranked 68th on the global ICT Development Index (IDI) for 2014, and 38th out of 40 European countries.

Poor infrastructure and a lack of electricity in certain areas, especially in the eastern and southeastern regions, have had a detrimental effect on citizens’ ability to connect to the internet, particularly from home.

According to the results of the Turkish Statistical Institute’s Household Usage of Information Technologies Survey, the number of households with internet access has risen to 69.5 percent. For individuals aged 16–74, the primary location of access is home (87.1 percent), followed by work (42.5 percent), and the homes of friends and relatives (37.7 percent). Wireless internet access in public places like shopping malls and airports was less frequently used (29.2 percent), followed by internet cafes (10.6 percent).

Mobile phone penetration in Turkey reached 95 percent in 2014, and all operators offer third-generation (3G) data connections. The mobile penetration rate exceeds 100 percent when the youngest

age group (0–9 years) is excluded. In the first three months of 2014, 58 percent of users accessed the internet via their phones. Computer and internet access rates for individuals aged 16–74 were recorded at 53.5 percent for computers and 53.8 percent for internet access in 2014. The rates among male participants were higher, at 62.7 percent and 63.5 percent, than among females, at 44.3 percent and 44.1 percent, respectively. Male users make up 56 percent of internet users in general. The annual growth rate in the total number of internet subscribers reached 22.6 percent in the first quarter of 2015.\(^\text{13}\) Total mobile internet usage increased 16 percent, and the number of internet subscribers increased by 3.4 percent, in the second quarter of 2015.\(^\text{14}\)

While prices have decreased, they do remain high in comparison with the minimum wage. Turkey does not report or share statistics on technical literacy, but data from the Turkish Statistical Institute (TÜİK) hint at a lack of familiarity with ICTs, particularly among older citizens.

**Restrictions on Connectivity**

Turkey's internet backbone is run by TTNET, a subsidiary of Türk Telekom that is also the largest internet service provider (ISP) in the country. Türk Telekom, which is partly state owned, has 202,098,723 km of fiber-optic infrastructure, while other operators having a combined total of just 54,730 km. Nearly 124,186 km of this infrastructure is used as backbone, with the remainder dedicated to access distribution.\(^\text{15}\)

Turkey does not have Internet Exchange Points (IXPs) that comply with international standards. However, there are two IXP models owned by private companies, both of which are in Istanbul: IST-IX, established by Terramark in 2009, and TNAP, established by seven leading ISPs in 2013. DEC-IX, a German internet exchange company, has announced that it will “open an internet exchange in Istanbul, to provide a neutral interconnection and peering point for internet service providers from Turkey, Iran, the Caucasus region and the Middle East.”\(^\text{16}\) According to the announcement, DEC-IX Istanbul will become operational within the third quarter of 2015.

On March 31, 2015, Turkey suffered a 10-hour power cut in almost all areas of the country. Authorities, including the prime minister and the energy minister, stated that they were investigating whether the power outage was due to a technical failure or a cyberattack, but a thorough explanation was never provided.\(^\text{17}\)

**ICT Market**

There are 672 operators providing ICT services in the Turkish market, and a total of 1,105 were authorized as of August 2015, according to the BTK.\(^\text{18}\) There are around 411 ISPs, though the majority

---


\(^\text{15}\) “Electronic Communications Market in Turkey – Market Data (2015 Q2),” slides 13 and 34.


\(^\text{17}\) “Major power outage plunges Turkey into chaos for hours,” Today’s Zaman, March 31, 2015, http://bit.ly/1iwnCKF.

Turkey

act as resellers for Türk Telekom. TTNET, founded in 2006 by Türk Telekom, dominates the ISP market with 74.3 percent of subscribers.\(^{19}\)

Turkcell is the leading mobile phone provider, with 47.1 percent of subscribers, followed by Vodafone and Avea.\(^{20}\) Although the BTK originally set a May 26 deadline for the auction of 4G spectrum, in April 2015 it was announced that the tender could be canceled due to President Erdoğan’s insistence that Turkey jump directly from 3G to 5G.\(^{21}\) An auction of 4G frequency bands was later held in August, but the BTK dubbed it “4.5G” in what some said was an effort to placate President Erdoğan.\(^{22}\)

Though all legal entities are allowed to operate an ISP, there are some requirements to apply for authorization, pertaining to issues like the company’s legal status, its scope of activity, and its shareholders’ qualifications. Furthermore, implicit obstacles may prevent newly founded companies without political ties or economic clout from entering the market. ISPs are required by law to submit an application for an “activity certificate” to the BTK before they can offer services. Internet cafes are also subject to regulation. Those operating without an activity certificate from a local municipality may face fines of TRY 3,000 to 15,000 (US$1,335 to US$6,680). Mobile phone service providers are subject to licensing through the BTK.

Regulatory Bodies

Policymaking, regulation, and operation functions are separated by the basic laws of the telecommunications sector. The Ministry of Transportation, Maritime Affairs, and Communications is responsible for policymaking, while the BTK is in charge of regulation.\(^{23}\)

The BTK and the Telecommunication and Communication Presidency (TİB), which it oversees, are well staffed and have a dedicated budget. However, the fact that board members are government appointees is a potential threat to the BTK’s independence, and its decision-making process is not transparent. Nonetheless, there have been no reported instances of certificates or licenses being denied. The TİB also oversees the application of the country’s website blocking law and is often criticized by advocacy groups for a lack of transparency and its apparent lack of independence from the executive.

The Computer Center of Middle East Technical University has been responsible for managing domain names since 1991. The BTK oversees and establishes the domain-name operation policy and its bylaws. Unlike in many other countries, individuals in Turkey are not permitted to register and own domain names ending with the country extension .tr, such as .com.tr and .org.tr, unless they own a trademark, company, or civil society organization with the same name as the requested domain.

Terms for providing landline service were hardened with some procedural changes published in the

---

Turkey

Turkish government gazette on December 30, 2014. Also included in the announcement was the fact that licenses would be invalidated for service providers that failed to integrate the new procedures.24

Limits on Content

Limits on content continued to increase in Turkey over the past year, with new amendments to the problematic Law No. 5651. Entire web platforms, including Facebook, Twitter, YouTube, and WordPress, were temporarily blocked and remain under intense pressure to promptly remove content when asked by Turkish authorities. Journalists, scholars, and public figures who are critical of the government faced coordinated harassment on Twitter. Despite these negative trends, users increasingly rely on online publications as a primary source of news, and a number of tools for citizen journalism and government accountability are gaining prominence.

Blocking and Filtering

 Blocking continues to increase steadily in Turkey. According to the reports of the independent organization Engelli Web, as of May 2015 over 80,000 websites were banned based on civil code–related complaints and intellectual-property rights violations. The number of blocked websites has risen from 43,785 to 81,525 in two years.25 This figure includes numerous sites that were blocked for political or social reasons, such as news outlets or online communities that report on LGBTI (lesbian, gay, bisexual, transgender, and intersex) issues, ethnic minorities, anti-Muslim content, or social unrest.

A number of platforms were blocked during the coverage period, frequently for refusing to restrict Turkish users’ access to specific pages or posts. In some cases, companies were not informed of the order or were not given sufficient time to comply. For example, on March 19, 2015, a Turkish court banned access to a single post on the blog-hosting service WordPress. As the site employs HTTPS, a connection method that makes blocking a single page technically very difficult, a second order called for the blocking of the entire WordPress.com domain.26 Access was later reinstated, but a similar incident occurred in July 2015 over five WordPress-hosted sites on Kurdish politics. In a blog post on its transparency page, WordPress’s parent company, Automattic, explained that one of the sites targeted by the TIB for allegedly supporting terrorism actually featured content that was critical of the Kurdistan Workers’ Party (PKK), a Kurdish militant group that is classified as a terrorist organization by Turkey, the United States, and a number of other governments.27

Facebook, Twitter, and YouTube were briefly blocked in April 2015 after two members of the left-wing terrorist organization Revolutionary People’s Liberation Party–Front (DHKP/C) took a public prosecutor hostage in his office in Istanbul on March 31. Prosecutor Mehmet Selim Kiraz was held for several hours before a failed rescue effort by Turkish security forces ended in the death of both the hostage and the perpetrators. After a photo showing one of the terrorists pressing his gun against Kiraz’s head went viral, the government issued an immediate gag order on all news of the incident. The Istanbul 1st Criminal Court of Peace banned access to 166 URLs that published the photo,

---

25 Engelli Web, “Kurum Bazinda Istatistikler.”
26 Efe Kerem Sozeri, “Ban against a single blog post leads Turkish ISPs to censor all of WordPress,” The Daily Dot, April 1, 2015, http://bit.ly/1lEk1WM.
as well as news and videos on Kiraz. The order included 78 news items, 54 Twitter statuses, 10 Twitter accounts, 16 YouTube videos, and 4 Facebook photos.28

Twitter responded to the court order within five hours by sending emails to at least 60 users, stating that “in order to avoid being completely banned in Turkey, we have withheld your status / your account.” Users reported that Facebook and YouTube were also temporarily inaccessible in Turkey. However, Facebook and Google, which owns YouTube, complied with the court order quickly enough to avoid a significant service outage.29 Similarly, Facebook, YouTube, and Twitter were blocked briefly on July 22, 2015, until they complied with court orders to remove images and videos related to the deadly bombing of a pro-Kurdish protest in the southeastern city of Suruç.30

The blocking and removal of online content (see “Content Removal” below) is regulated under Law No. 5651, whose full name is “Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication.”31 It was initially established in 2007 to protect children and prevent access to illegal and harmful internet content. This includes material related to child sexual abuse, drug use, the provision of dangerous substances, prostitution, obscenity, gambling, suicide promotion, and crimes against Mustafa Kemal Atatürk, the founding father of modern Turkey.32 The responsibilities of content providers, hosting companies, public access providers, and ISPs are delineated in Law No. 5651. Domestically hosted websites with proscribed content can be taken down, while websites based abroad can be blocked and filtered through ISPs. The law has already been found to be in contravention of the European Convention on Human Rights.

One of the main legal developments over the past year in Turkey was the passage of amendments to Law No. 5651 that broadened the scope for censorship, increasing rather than addressing the law’s problems in the wake of public criticism.33 A set of amendments enacted in March 2015 authorized cabinet ministers to order the TIb to block content when necessary to “defend the right to live, secure property, ensure national security and public order, prevent crime, or protect public health.” The orders are then taken up within four hours by the TIb, which must also submit the decision to a criminal court within 24 hours. If a judge does not validate the decision within 48 hours, the blocking order must be rescinded.34 A similar bill passed in September 2014 had been overturned by the Constitutional Court in October of that year.

Separate amendments to the law had been enacted earlier in 2014. While the original version of Law No. 5651 included only notice-based liability and takedown provisions for content that violates individual rights, changes passed in February 2014 extended this provision to include URL-based

Turkey

blocking orders to be issued by a criminal court judge. The February 2014 amendments also entrusted the TİB with broad discretion to block content that an individual or other legal claimant perceives as a violation of privacy, while failing to establish strong checks and balances. These changes came after leaks of the alleged phone conversations of top government officials on December 17, 2013, and they laid the groundwork for the eventual blocking of social media platforms such as Facebook, Twitter, and YouTube. Access to Bitly, Imgur, and Tumblr was also temporarily blocked during the coverage period. TİB authorities later restored access to Bitly and explained that the site had been banned due to a technical error.35

The February 2014 amendments to Law No. 5651 also shield TİB staff if they commit crimes during the exercise of their duties. Criminal investigations can only be initiated through an authorization from the TİB director for TİB staff, and from the relevant minister for the TİB director. This process casts serious doubt on the functioning and accountability of the TİB. ISPs are required to set up a new Association for Access Providers, membership in which is compulsory in order to obtain an “activity certificate” to legally operate in the country. ISPs must also comply with blocking orders from the TİB within four hours or face a penalty of up to TRY 300,000 (US$103,000). Failure to take measures to block all alternative means of accessing the targeted site, such as proxy sites, may result in a fine of up to TRY 50,000 (US$22,000).36

Currently, access to a number of well-known sites and services is blocked, including Metacafe. SoundCloud was blocked in January 2014 following the dissemination of audio leaks allegedly implicating Erdoğan and his inner circle in corruption.37 An article by columnist Ezgi Başaran—in which she criticized the rector of Istanbul Technical University for ordering the removal of trees that were planted in memory of citizens who died during the Gezi Park protests in 2013, increasing the number of security guards on campus, and failing to open the social sciences faculty—was blocked on October 1, 2014, without notice to either Başaran or the article’s publisher, Radikal.com.38

The courts have indefinitely blocked access to the websites of several alternative news sources that report news on southeastern Turkey and Kurdish issues, such as Atılım, Özgür Gündem, Azadiya Welat, Keditör, Günlik Gazetesi, and Fırat News Agency. Within the list of hundreds of blocked domains and internet protocol (IP) addresses, there are also examples of websites that were targeted for unclear reasons, such as todocolleccion.net, a Spanish auction website; various foreign e-commerce websites featuring lingerie and bikinis; and roncalli.org, the website of a Catholic high school.39 The minister of family and social policy has also stated that the highly popular game Minecraft should be investigated and banned for encouraging children to commit violence.40

Despite the fact that it is not illegal, sexually explicit content is often blocked by the authorities under the pretext of protecting minors, including 5Posta, a Turkish-language website that features writings of a sexual nature, and the Playboy website. 5Posta is blocked under two different decisions, and an appeal is ongoing.41 An individual petition was separately lodged with the Constitutional

41 Ankara 8th Administrative Court Decision No 2010/3103, dated 18 October 2012; Ankara 8th Criminal Court of Peace
Turkey

Court by the owner of 5Posta in November 2013. Similarly, university professors Yaman Akdeniz and Kerem Altparmak lodged an appeal at the Council of State against the Playboy blocking in early 2014. The two professors had also appealed to unblock Scribd, which is now accessible. Grindr, a mobile application that uses location data to connect gay, bisexual, and bicurious men, became the first app to be rendered inaccessible from Turkey in August 2013. The Istanbul 14th Criminal Court of Peace blocked it as a “protection measure.” The ban also covers the application’s website. Grindr had over 125,000 monthly active users at the time.42

Furthermore, Turkey has censored atheist and anti-Muslim websites deemed defamatory, according to a court order dated February 27, 2015.43 The latest bans came after the government appealed to a local court, citing blasphemy provisions in the criminal code. The Ankara Gölbasi Criminal Court of Peace issued an order to ban 49 URLs, including atheist and anti-Muslim websites; the French satirical magazine Charlie Hebdo and its corresponding Wikipedia entry; and Turkish and foreign news articles about a controversial Charlie Hebdo cover that caricatured the Muslim prophet Muhammad.44 However, websites that support radical Islamist groups such as the Islamic State and Al-Qaeda have not been subject to blocking through court orders. For example, takvahaber.net, enfalmedya.com, and mustaqim.net, which call on Muslims to join these illegal organizations and openly disseminate their propaganda, are not blocked in Turkey.45

The vast majority (93.4 percent) of blocking orders are issued by the TİB,46 rather than court orders.47 The procedures surrounding decisions are nontransparent in both cases, creating significant challenges for those seeking to appeal. Judges can issue blocking orders during preliminary investigations as well as during trials. The reasoning behind court decisions is not provided in blocking notices, and the relevant rulings are not easily accessible. As a result, it is often difficult for site owners to determine why their site has been blocked and which court has issued the order. The TİB’s mandate includes executing judicial blocking orders, but it can also issue administrative orders for foreign websites, content involving sexual harassment of children, and obscenity. Moreover, in some cases it successfully asks content and hosting providers to remove offending items from their servers, in order to avoid issuing a blocking order that would affect an entire website. This occurs despite the fact that intermediaries are not responsible for third-party content on their sites.

In addition to these blocks, ISPs offer “child” and “family” filtering options under rules established by the BTK in 2011, though the filtering criteria have been criticized as arbitrary and discriminatory.48 The BTK tried to mandate filtering for all users in 2011,49 but withdrew the proposal following a legal

---

43 Gölbasi Criminal Court of Peace Decision No 2015/191 D.Is, dated February 27 2015.
47 According to TİB statistics from May 2009, the last date these were available, the courts are responsible for 21 percent of blocked websites, while 79 percent are blocked administratively by the TİB. Reporters Without Borders, "Telecom Authority Accused of Concealing Blocked Website Figures," May 19, 2010, http://en.rsf.org/turkey-telecom-authority-accused-2010-05-19,37511.html.
Turkey

The child filter obstructs access to Facebook, YouTube, Yasam Radyo (Life Radio), the Armenian minority newspaper Agos, and several websites advocating the theory of evolution, even as some anti-evolution websites remain accessible. The filtering database is maintained by the government without clear criteria. A “Child and Family Profiles Criteria Working Committee” was introduced to address this problem in 2012, but it was largely made up of BTK members or appointees and does not appear to be active.

Internet access is filtered at primary education institutions and public bodies. The Ministry of Education received public criticism for blocking access to a number of minority news websites in January 2012. In response to questions from lawmakers, the ministry acknowledged that it uses Fortiguard web filtering software at primary education institutions. In a separate written response to parliament member Ibrahim Binici dated February 27, 2012, the administrators of the Turkish parliament stated that internet access within parliament was filtered and that access to gambling, pornographic, gaming, and terrorist websites was blocked. In December 2012, they rejected claims that access to websites pertaining to the Alevi Muslim minority was among the blocked content. However, the Alevi Culture Association’s website, alevikulturdernekleri.com, was filtered in the parliament in December 2014. Sezgin Tanrikulu of the opposition Republican People’s Party (CHP) asked the government about the filtering via a parliamentary question, and the assembly’s deputy chairman, Sadik Yakut, responded that the site was blocked due to an error of misclassification.

Content Removal

In addition to widespread filtering, state authorities are proactive in requesting the deletion or removal of content. Social media platforms comply with administrative decisions and court orders as promptly as possible for fear of being banned. Twitter responded to a court order about the attack on Prosecutor Kiraz within five hours, and all online news sources deleted their tweets together with their articles about the incident at once. Popular Turkish websites are also subject to content removal orders. Courts issued several orders pertaining to user-generated content websites such as Eksi Sozluk (Sour Dictionary), Inci Sozluk (Pearl Dictionary), and ITU Sozluk (Istanbul Technical University Dictionary).

In January 2015, Turkish officials threatened to shut down Twitter unless the company took down the account of Birgün, a left-wing newspaper, which had circulated documents about a military police raid on National Intelligence Organization (MIT) trucks that were traveling to Syria and allegedly carrying weaponry. The Adana Criminal Court of Peace issued an order stating that publication of the information about the trucks violated national security and interfered with a continuing investigation, and that the blocking was necessary for the purpose of “preventing the violation of the personal

---

50 On September 27, 2011, the Council of State rejected the “stay of execution” request by BIAnet referring to the annulment of the February 22, 2011.
53 See response to Ibrahim Binici dated February 27, 2012, TBMM response no. A.01.0.K KB.0.10.00.00-120.07(7/3747)-79795-50631.
Turkey

rights of MIT as a legal entity by publishing such information."56 Twitter and Facebook complied with the court order accordingly. Twitter removed the content and suspended accounts that shared the information about the trucks. However, several Twitter users, Birgün in particular, continued to challenge the ban by posting screenshots of their deleted tweets and leaked legal documents. While Twitter took steps to comply with the court decision, it refused to suspend Birgün’s account.

According to Twitter’s latest Transparency Report,57 requests by the Turkish authorities to remove content have increased dramatically since Twitter started publishing data in 2012. The total number of removal requests—by courts as well as government agencies and the police—rose from 2 in the period of July to December 2013 to 186 in the six months afterward, during the height of the corruption allegations and intelligence leaks. The figure continued to grow, reaching 477 in the second half of 2014 and 718 in early 2015. Incredibly, 92 percent of all court orders and 55 percent of administrative requests that Twitter received around the world over the past six months originated in Turkey alone.58 Twitter reported that some content was duly withheld in 34 percent of cases.

Of 376 court orders seeking the removal of content, 328 came from Turkey in the period July 1 to December 31, 2014. Another 149 requests came from Turkish government, police, and other institutions in the same period, out of the global total of 420 from such entities. A total of 2,642 Turkish accounts were identified in the official requests, of a global total of 3,236. In response to the Turkish requests, Twitter withheld 62 accounts and 1,820 tweets. Overall, Twitter withheld 85 accounts and 1,982 tweets from around the world.59 On January 20, 2015, two weeks before the publication of the late-2014 report, free speech activists and professors Kerem Altıparmak and Yaman Akdeniz sent a formal notice to Twitter,60 emphasizing the company’s obligation to respect human rights.61

According to Facebook’s Government Requests Report, in the second half of 2014 the company restricted 3,624 pieces of content, on orders from both the BTK and Turkish law enforcement, particularly in compliance with Law No. 5651.62 In recent years, Facebook has been criticized by pro-Kurdish movements for removing several pages related to the groups, as well as some used by antigovernment activists.63

Media, Diversity, and Content Manipulation

The climate of fear created by widespread government prosecution of online activities has led to an increase in self-censorship, particularly when it comes to criticism of the government or public officials. Speech on Islam or the prophet Muhammad can result in death threats and legal battles. Online posts about the “Kurdish problem” and Turkish-Armenian relations have become less controversial in recent years, but they remain sensitive, particularly during periods of ethnic tension and violence in the southeast.

56 Adana 5th Criminal Court of Peace Decision No. 2015/197 DIs, dated January 14, 2015.
Turkey

Turkish users increasingly rely on internet-based publications as a primary source of news, and despite the country’s restrictive legal environment and growing self-censorship, the Turkish blogosphere is still surprisingly vibrant and diverse. There are a wide range of blogs and websites through which citizens question and criticize Turkish politics and leaders, including on issues that are generally viewed as politically sensitive. The majority of civil society groups maintain an online presence.

Journalists and scholars who are critical of the government have faced orchestrated harassment on Twitter, often by dozens or even hundreds of users. Reports from Turkish media in September 2013 indicated that the AKP had enlisted some 6,000 volunteers to set the agenda on social media, counter government critics, and drive discussions on important foreign policy issues. The AKP government has also allegedly hired thousands of Twitter users to intimidate antigovernment commentators. CHP İzmir deputy Erdal Aksunger claimed in a parliamentary question in November 2014 that the MIT is subcontracting a group of 150 people known as "Ak Troller" (white trolls) who are believed to work as Twitter trolls for the AKP. Despite its hostile attitude toward online speech, the AKP changed its digital strategy during the 2015 general elections campaign, creating a headquarters called the New Turkey Digital Office. AKP deputy chairman and spokesman Beşir Atalay described the party’s new digital office as “an important communication platform that will be useful after the elections, too.”

Although a large number of websites are blocked, circumvention tools are widely available, enabling even inexperienced users to avoid filters and blocking mechanisms. Each time a new order is issued and a popular website is blocked, articles are published to instruct users on how to access it. YouTube was the eighth-most-accessed site in Turkey in 2010, at a time when it was officially blocked. However, when internet users employed Google’s Domain Name System (DNS) service and OpenDNS to evade blocks on both Twitter and YouTube in 2014, Google announced that it had received several credible reports and confirmed with their own research that Turkish ISPs had intercepted and hijacked the settings.

According to IAB Turkey Internet Audience Measurement, the most visited online news source is milliyet.com.tr, the online edition of the newspaper Milliyet. Hurriyet, an influential newspaper with a readership of almost 2 million, is the second-most-visited online news source. Nonetheless, new models for citizen journalism and volunteer reporting are also gaining traction, such as 140journos, dokuz8haber (nine eight news), and Otekilerin Postasi (The Others’ Post). Independent news sources such as bianet.org, diken.com.tr, and t24.com.tr are also popular. In general, the online environment remains more free and diverse than traditional media. Turkish mainstream media largely failed to report on the Gezi Park protests; instead, YouTube, Facebook, and Twitter arose as some of the few outlets for reliable coverage on the protests, leading Erdoğan to describe social media as “the worst menace to society.”

Turkey

Digital Activism

After the highly popular Occupy Gezi protests in 2013, environmentalist demonstrations were mounted against government moves to construct a mosque in Istanbul’s protected area of Validebağ Grove, and against the felling of 6,000 olive trees for the construction of a power plant in the village of Yirca in late 2014. Hashtags such as #validebag, #yirca, and #sendeanlat (tell your story) were popular during the coverage period, with the third attracting over 500,000 tweets within two days to spread awareness of violence against women after the brutal rape and killing of 20-year-old university student Özgecan Aslan. Thousands of women posted pictures of themselves laughing after Deputy Prime Minister Bülent Arınç stated in July 2014 that women should not laugh out loud in public.

Before important elections in 2014 and 2015, a number of initiatives were established to monitor ballot boxes and prevent election fraud. Among these was Oy ve Ötesi (Vote and Beyond), the first civic election-monitoring initiative, which managed to enlist more than 55,000 active volunteers from all walks of society via social media outreach. Most recently, the initiative monitored 128,620 of 174,400 ballot boxes in 46 provinces and 173 counties during the general elections in June 2015.

Violations of User Rights

As social media have gained prominence as a tool for activism and criticism of the government, legal cases against Facebook and Twitter users have skyrocketed. Prison sentences are rare, but the constant legal intimidation has a chilling effect on free speech online. Surveillance remains a key issue amid the fallout from high-level corruption scandals and intelligence leaks in 2013 and 2014, and leaks from mid-2015 revealed that a civilian police directorate possessed malware products from the Italian company Hacking Team. On a positive note, there were fewer instances of physical attacks against citizen journalists covering protests, although online harassment has persisted.

Legal Environment

The Turkish constitution includes broad protections for freedom of expression. Article 26 states that “everyone has the right to express and disseminate his thought and opinion by speech, in writing or in pictures or through other media, individually or collectively.” Turkish legislation and court judgments are subject to the European Convention on Human Rights and bound by the decisions of the European Court of Human Rights. The constitution also seeks to guarantee the right to privacy, though there are limitations on the use of encryption devices, and surveillance by security agencies

73 For an interview with the creator of the hashtag, see Efe Kerem Sözeri, “#sendeanlat Tag Starter Speaks Up,” BIANet, February 17, 2015, http://bit.ly/1Knmv5Q.
Turkey

is highly prevalent. There are no laws that specifically criminalize online activities like posting one’s opinions, downloading information, sending email, or transmitting text messages. Instead, many provisions of the criminal code and other laws, such as the Anti-Terrorism Law, are applied to both online and offline activity.

One notable development from the coverage period was the passage of the Homeland Security Act on March 27, 2015. Although the final version of the bill did not contain some of the most exorbitant restrictions, civil society and free speech advocates still expressed fears that the law would be used to suppress online news sources, particularly ahead of important parliamentary elections.78

Prosecutions and Detentions for Online Activities Turkish users face widespread legal prosecution and detention for their online activities, though long prison sentences are less common. Over the past year, dozens of Twitter users, some with only hundreds of followers, were subject to prosecution, mostly on charges of insulting government officials. Erdoğan has filed criminal complaints against at least 67 people for “insulting” him online since he was elected president in August 2014.79 In addition to journalists, students have increasingly been prosecuted for defamation.

There were many ongoing investigations or trials during the coverage period, including the following:

- Journalist and anchorwoman Sedef Kabaş was detained and police raided her home after one of her tweets in December 2014 alluded to a cover-up of a governmental corruption scandal. She faced up to five years in jail for tweeting, “Do not forget the name of the prosecutor who dismissed the Dec. 17 case.”80 Kabaş was released pending trial and eventually acquitted in October 2015 of “targeting individuals involved in the fight against terrorism.”81

- Journalist and writer Aytekin Gezici was detained in October 2014 in Adana after a police raid on his home. His recent tweets had criticized Erdoğan, Arınç, and former justice minister Bekir Bozdağ on Twitter.82 In September 2015, he received a prison sentence of five years and nine months, as well as a judicial fine equivalent to one year and nine months in prison, for “insulting” the three public figures.83

- Kamil Maman, a reporter for Bugün newspaper, faces 25 separate investigations for critical tweets published in the past six months about the government, particularly Davutoğlu and Erdoğan. Maman could receive a combined total of 130 years in prison.84

- Ten journalists were being prosecuted in mid-2015 for tweets that the government considered “propaganda in support of terrorist organizations” in connection with the attack on

---

79 Finkel, “Miss Turkey on Trial for Allegedly Insulting President Erdogan.”
Prosecutor Kiraz by two militants. The journalists faced up to five years in prison if found guilty.85

• Yaşar Elma, a journalist from a local daily newspaper, received a suspended prison sentence in April 2015 for “liking” a Facebook post that was critical of Erdoğan and deemed “insulting” by the court.86

• Mehmet Baransu, a journalist linked with the Islamist movement of Fethullah Gülen, which has become an opponent of the AKP government, was subjected to a criminal case in late 2014 for “insulting and blackmailing” Erdoğan on Twitter. He faces up to seven years in prison if found guilty.87

• Prime Minister Davutoğlu sued U.S.-based analyst Cenk Sidar, a writer for the online news source diken.com.tr, over an opinion piece accusing Davutoğlu of hypocrisy for joining a freedom of expression march in Paris following the terrorist attack on Charlie Hebdo in January 2015.88

• On February 27, 2015, a 13-year-old student in western Turkey was taken from his classroom to be questioned on suspicion that he “insulted” Erdoğan on Facebook. The prosecutor had yet to decide whether he would file a criminal case.89

• Also in February, 19-year-old university student Arif Buğra Aydoğan was arrested for tweeting “thief, murderer Erdoğan.” Two others, Kadir Yavaş and Şafak Kurt, were later arrested on similar charges while protesting against Aydoğan’s arrest.90

• In April, 20-year-old university student Meral Tutcalı received a suspended sentence of one year in prison for “insulting a public official” over a satirical tweet. Tutcalı quoted a satirical news article in the tweet, which referred to the governor of Adana as more important than the president.91

• Former Miss Turkey Merve Büyüksaraç was put on trial in 2015 for using her Instagram account to share a satirical poem about Erdoğan’s corruption scandal that had originally appeared in the Turkish comic Uykusuz.92 The model faces up to two years in prison.

• Turkish singer Atilla Taş was questioned for “insulting” Davutoğlu on Twitter on March 6, 2015.93

While the number of court cases against users is staggering, the majority of cases do not result in

Turkey

jail time. For example, 29 individuals faced up to three years in prison for tweets that called on users to join the Gezi protests in 2013, often by simply providing the location of the protests.94 In the last hearing on September 22, 2014, 27 of the accused were acquitted of all crimes, one defendant was fined TRY 8,000 (US$2,750) for “insulting the prime minister,” and another’s file was set aside for a future date.95

Nonetheless, journalists and government critics do face prison time in Turkey, often on trumped-up charges related to their offline activities. One such case centers on Sevan Nişanyan, an ethnic Armenian writer and public intellectual who criticized the government’s attempts to prohibit criticism of the prophet Muhammad. Nişanyan has been in prison since January 2014 based on an earlier conviction for violating the Code of Protection of Cultural and National Properties by undertaking construction on his own property;96 he is currently the only person imprisoned in Turkey for violating the code.97 He faces further time behind bars in several pending cases on charges such as “disrespecting the religious belief of a group,” under Article 216 of the criminal code. Other charges stem from posts on his personal blog about the Armenian genocide, and about Atatürk, whom the writer described as a “fascist dictator.”

Surveillance, Privacy, and Anonymity

The abuse of government surveillance, the bulk retention of user data, and measures to prevent encryption and anonymity are all concerns in Turkey. Leaked emails revealed a contract between the Italian surveillance software company Hacking Team and the General Directorate of Security (GDS), a civilian police force, for the use of Hacking Team’s “Remote Control System” from June 2011 to November 2014.98 Under Turkish law, the interception of electronic communications falls under the purview of the TİB, and questions remain over the legality of the GDS using software that can infiltrate targets’ computers. The prominence of so-called Gülenists in the police and judiciary has been a major point of discussion in the country in recent years, particularly after leaked wiretaps widely attributed to such officials led to the government corruption scandals of 2013 and 2014.

The scandals have prompted high-level sackings and reshuffling within the police and judiciary, apparently aimed at removing suspected Gülenist officials. On January 20, 2015, a public prosecutor’s office issued arrest warrants for 28 officials both from the TİB and the Scientific and Technological Research Council of Turkey (TÜBİTAK), including the former deputy chairman of TİB, Osman Nihat Şen, and former TÜBİTAK vice president Hasan Palaz. The officials were accused of “spying,” “destroying the union of the state,” and “unauthorized listening of cryptographic and ordinary phones,” as well as “being a member of armed terrorist organization, procurement of state secrets with aim of political and military espionage, attempting to remove the government of Republic of Turkey or preventing it from performing its duties, violation of the privacy of communications, and damaging, destruction of, or making inaccessible a system of data processing.”100 President Erdoğan, Minister

97 “Jailed Turkish-Armenian journalist Nişanyan’s sentence raised to 11 years,” BGN News, April 19, 2015, http://bit.ly/1QGH6XT.
of Development Cevdet Yılmaz, former justice minister Sadullah Ergin, and former minister of family and social policies Fatma Şahin have been cited in the indictment as the complainants. According to the indictment, the suspects allegedly spied on encrypted phones without a court decision and held the recorded files in order to transfer them to the Gülen movement. Erdoğan had formerly denied the recordings’ authenticity. Osman Nihat Şen and other suspects were placed in pretrial detention.

According to Article 22 of the constitution, “everyone has the right to freedom of communication, and secrecy of communication is fundamental.” This right can only be violated under a court order in cases of “national security, public order, prevention of crime commitment, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law in cases where delay is prejudicial.” For the most part, any action that could interfere with freedom of communication or the right to privacy must be authorized by the judiciary. For example, judicial permission is required for technical surveillance under the Penal Procedural Law. Before the passage of the Homeland Security Act, in urgent situations the law allowed Turkish security forces to conduct intelligence wiretapping for 24 hours without a judge’s permission. However, with the new law the time limit increased to 48 hours, though the wiretapping officials are required to notify their superiors. In addition, only the Ankara high criminal court is authorized to decide whether the wiretapping is legitimate. Despite constitutional guarantees, most forms of telecommunication continue to be tapped and intercepted.

In April 2014, the parliament enacted a law that expanded the powers of the MIT. Law 6532 on Amending the Law on State Intelligence Services and the National Intelligence Organization grants intelligence agents unfettered access to communications data without a court order. The law forces public and private bodies—including but not limited to banks, archives, private companies, and professional organizations such as bar associations—to give the MIT any requested data, documents, or information regarding certain crimes, such as crimes against the security of the state, national security, state secrets, and espionage. Failure to comply is punishable by prison. In a clause related to the MIT’s ability to intercept and store private data on “external intelligence, national defense, terrorism, international crimes, and cyber-security passing through telecommunication channels,” no requirement to procure a court order is mentioned. The law also limits MIT agents’ accountability for wrongdoing. Courts must obtain the permission of the head of the agency in order to investigate agents, and journalists or editors who publish leaks on MIT activities via media channels may be imprisoned for three to nine years. Some observers have argued that the bid to shield the MIT from judicial investigations was intended to provide legal cover for the agency’s negotiations with the PKK, which is officially recognized as a terrorist organization; it also facilitated the crackdown on government opponents such as the Gülenists.

The CHP objected to the MIT law and filed an appeal with the Constitutional Court.

In 2013, the daily newspaper Taraf filed a complaint at the Constitutional Court against the MIT for illegally tapping journalists’ phones. Lawyers had initially filed a complaint with the Istanbul Public Prosecutor’s Office in 2012, but since MIT agents can only be prosecuted with the permission of the

101 The Constitution of the Republic of Turkey.
prime minister, the prosecutor’s office decided not to pursue the case. In May 2015 the Constitutional Court ruled that issuing such wiretapping orders was a violation of constitutional rights, particularly the right to privacy.

The constitution states that “secrecy of communication is fundamental,” and users are allowed to post anonymously online. However, the anonymous purchase of mobile phones is not allowed; buyers must provide official identification. According to a Council of Ministers decision dated 2000, only one mobile phone import per two years is permitted per person. Imported devices can be registered at mobile phone operators’ subscription centers and an e-government website, for a fee of TRY 131.50 (US$45). Devices that are not registered within 60 days are shut off from communications. In 2011, the BTK imposed regulations on the use of encryption hardware and software. Suppliers are required to provide encryption keys to state authorities before they can offer their products or services to individuals or companies within Turkey. Failure to comply can result in administrative fines and, in cases related to national security, prison sentences. Mobile phone companies are obliged to keep information on the number and identities of their users, call periods, and traffic data for one year.

Under Law No. 5651, hosting and access providers must retain all traffic information for one year and maintain the accuracy, integrity, and confidentiality of such data. In addition, access providers must file the data together with a time stamp and provide assistance and support to the TİB in monitoring internet traffic. Public-use internet providers hold different responsibilities depending on their status as either commercial or noncommercial. Commercial providers are defined as entities that provide internet service upon a certain payment, such as internet cafes. Noncommercial public-use internet providers are defined as entities that provide internet service at a certain venue for a certain period of time, such as in hotels and restaurants. While all public-use internet providers are expected to take measures to prevent access to criminal content and store internal IP distribution logs, the commercial providers must also receive permission from the local administration, use a content-filtering service approved by the TİB, and keep accurate daily records of internal IP distribution logs using software supplied by the TİB, which must be stored for a period of one year. In addition, these commercial providers are required to install a video surveillance system so as to identify users, and retain such records for seven days. All data must be made available to the TİB upon request—and without the need for a court order—under penalty of TRY 10,000 to 100,000 (US$4,400 to 44,000) in fines.

Turkey has yet to adopt a data-protection law, though September 2010 amendments to the Turkish constitution included data-protection provisions. It was expected that a draft data-protection bill would reach the parliament after the 2015 elections.

### Intimidation and Violence

Citizen journalists and reporters for online news outlets did not face physical violence in this coverage period, unlike in previous years, when journalists were harassed or injured while covering pro-

---

Turkey

tests. However, social media users—particularly public figures, journalists, and intellectuals—faced online harassment. In February 2015, the prime minister’s guards attempted to detain Young Civilians founder and academic Turgay Oğur outside a mosque due to his tweets criticizing their entry into the mosque while carrying machine guns as part of an escort for Davutoğlu.108

Technical Attacks

Popular news organizations such as Zaman, Today's Zaman, Cihan, Rotahaber, Radikal, Sözcü, and Taraf reported cyberattacks against their websites during the 2014 election period, a common occurrence in recent years. Internet access was suspended at the offices of Turkish-language Zaman and English-language Today's Zaman for several hours.109 On March 31, 2015, a massive power cut occurred in almost all 81 provinces. Many blamed the cut on a technical failure, while others attributed it to a cyberattack originating in Iran.110

In recent years, Turkish government sites have been attacked by hacktivist organizations like Anonymous.111 During 2012, the leftist Redhack group infiltrated several government websites and leaked confidential information. The group, which has over 675,000 followers on Twitter, hacked into the servers of the Ministry of Foreign Affairs, the Ministry of Finance, and the Turkish Higher Education Authority, among others, during 2012 and early 2013.112 Under a court order, Twitter made Redhack’s main Twitter accounts inaccessible from Turkey in 2014.

Uganda

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>34</td>
<td>36</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- Four individuals were arrested for their alleged involvement with Facebook pages known for critical commentary (see Prosecutions and Detentions for Online Activities).

- Government efforts to draft a Data Protection and Privacy Bill were seen as a positive step towards promoting the right to privacy, but the draft was later criticized for its broad and vague conditions in which personal data may be collected, thus leaving it open to misinterpretation and abuse (see Surveillance, Privacy, and Anonymity).

- Intimidation, threats of violence, and technical attacks against vulnerable groups and marginalized communities, particularly the LGBTI community, were frequent online (see Intimidation and Violence and Technical Attacks).
Introduction

Internet penetration continues to grow in Uganda, connecting more citizens to new digital media tools and platforms, particularly on internet-enabled mobile devices, in urban and rural areas alike. In recognition of the internet’s powerful potential to enhance economic growth, the government has invested considerable resources in the development of information and communications technology (ICT) infrastructure and networks, resulting in increasing access for a growing community of netizens. Social media applications such as Facebook, WhatsApp, and Twitter have become significant platforms on which Ugandans connect with each other, share information, and consume the news.

While traditional press freedom in Uganda is persistently under pressure from the government, internet freedom has not been subjected to the same level of pressure or threat. Instead, threats to internet freedom in Uganda during the coverage period took the form of increasing arrests of users for their online activities. In November 2014, three activists in western Uganda were arrested for allegedly inciting violence on the Masindi News Network (MANET) Facebook group, which disseminates information about the western region of the country to over 16,000 members and often posts demands for political accountability from the government. In February 2015, a man named Robert Shaka was summoned by police and subsequently arrested on suspicions of running the popular Facebook account called Tom Voltaire Okwalinga (TVO), which is well known for its politically charged posts that often accuse the Ugandan president and other senior leaders of corruption and incompetence. Shaka was arrested again in June 2015 on charges of disseminating “offensive communication” under the 2011 Computer Misuse Act for posts on the TVO Facebook page.

In mid-2015, the Uganda Police Force’s Cyber Crimes Unit, established in 2014, publicly stated that its efforts to crack down on cybercrimes include “threats that could destabilize the country” committed on social media platforms. Observers noted the government’s increased crackdown on online speech, particularly on social media platforms, in the past year may be an indication of restrictions to come in the lead up to the presidential election in 2016. Meanwhile, intimidation, threats of violence, and technical attacks against vulnerable groups and marginalized communities, particularly the LGBTI community, were frequently reported and remained a growing concern in Uganda in 2014-2015.

Obstacles to Access

ICTs continued to expand across Uganda over the past year, resulting in increased access to both internet and mobile phone services. Despite increased industry competition the cost of access remains relatively high for the majority of Ugandans, especially those in rural areas.

Availability and Ease of Access

In 2014-2015, internet access continued to grow in Uganda with a reported internet penetration rate of 18 percent, up from 16 percent in 2013, according to the International Telecommunication Union. Nonetheless, access to broadband internet is still rare and available mostly in urban areas, with less than 1 percent of the population estimated to have fixed-line broadband subscriptions in 2014. Internet speeds are still slow, averaging just over 1.5 Mbps (compared to a global average

of 4.5 Mbps), according to data from Akamai’s “State of the Internet” 2014 fourth quarter report. Meanwhile, mobile phone penetration stood at 52 percent in 2014, a slight increase from 48 percent in 2013.

Many Ugandans access the internet at cybercafes where it costs less than US$1 for an hour of browsing. Internet access via mobile broadband is also becoming increasingly popular—reaching 12 percent of the population in 2014—due to the growing availability of cheap mobile internet bundles. An hour of mobile web browsing (equating to approximately 10 Mb of data) costs UGX 300 (US$0.10), while a limited monthly bundle of 1 GB costs between UGX 35,000 and 42,000 (US$12-16). Meanwhile, 10 GB of an unlimited mobile broadband connection can cost UGX 125,000 (US$43) for one month and over US$259 for six months.

While increasing market competition has continued to drive down costs, particularly on mobile phones, internet-enabled devices cost an average of US$50, which is still high for the majority of Ugandans. A January 2015 survey by the regulator found internet access is still very expensive for both rural and urban users.

Limited access to electricity further impedes access to ICTs. The national electricity distributor reports a customer base of just over 650,000, most of whom are located in urban areas, and alternative power sources, such as fuel-powered generators and solar energy, are very costly. Meanwhile, only 18 percent of Ugandans live in urban areas, resulting in a significant urban-rural divide in access.

The government, through the Rural Communications Development Fund (RCDF), aims to establish computer centers in all of its educational institutions across the country, provide access to basic communications services to all Ugandans, leverage investments for rural communications, and promote overall ICT usage. The fund further supports the establishment of internet cafes, internet points of presence (which are rural wireless connectivity networks with a 5 to 10 km radius with costs, speeds and types of services comparable to those in the capital city, Kampala), ICT training centers, and web portals for local government districts. By the end of 2014, 100 school ICT laboratories had been established.

Restrictions on Connectivity

There were no reported disruptions in ICT connectivity during the coverage period.

---

6 On the Vodafone Uganda Network.
7 Cartesian, Broadband Internet Access from a Mobile Terminal.
Uganda

Uganda’s backbone connection to the international internet is privately owned in a competitive market. The country’s national fiber backbone is connected to the EASSy international submarine fiber-optic cable system that runs along the east and southern coasts of Africa. Telecommunications providers are also hooked to TEAMS (The East African Marine System) and SEACOM marine fibers through Kenya.

Since 2007, Uganda’s ICT ministry through the National Information Technology Authority – Uganda (NITA –U) has been developing the National Data Transmission Backbone Infrastructure, which aims to ensure the availability of high bandwidth data connections in all major towns at reasonable prices. As of early 2015, the project has completed the installation of 1,400 kilometers connecting 27 district headquarters.

ICT Market

The number of industry players has grown over the years, and many now offer comparable prices and technologies. There are no known obstacles or licensing restrictions placed by the government on entry into the ICT sector, and new players have entered the market with ease in recent years. Currently, there are 34 telecommunications service providers that offer both voice and data services. Aside from the state-owned Uganda Electricity Transmission Company Limited, which is a licensed public infrastructure provider that has part ownership of Uganda Telecom, all of the licensed service providers are privately owned.

In February 2015, Vodafone launched in Uganda, joining a competitive market dominated by bigger, well-established telecommunications brands, such as MTN Uganda, Uganda Telecom, Airtel, Smart Telecom, and Africell Uganda (former Orange Uganda). All of these telecoms offer 4G LTE network speeds. Meanwhile, 17 ISPs were connected to the Uganda Internet Exchange Point (UIXP) as of mid-2015.

Regulatory Bodies

Uganda’s telecommunications sector is regulated by the Uganda Communications Commission (UCC), which is mandated to independently coordinate, facilitate, and promote the sustainable growth and development of ICTs in the country. The UCC also provides information about the regulatory process and quality of service, and issues licenses for ICT infrastructure and service providers.

Uganda

The commission’s funds come mainly from operator license fees and a 2 percent annual levy on operator profits.

There is a general perception, however, that comprehensive and coherent information about the commission’s operations is not always accessible, and that the body is not entirely independent from the executive branch of the government. For example, the ICT minister has the authority to approve the new regulator’s budget and appoint members of its board with approval from the cabinet. There are no independent mechanisms in place to hold the regulator accountable to the public.

Limits on Content

There were no reported incidents of direct government interference with internet content during the coverage period, though the government indicated its intent to shut down certain platforms in the face of growing criticism disseminated online. A popular opposition Facebook page was taken down in January 2015 for breaching Facebook’s terms of service; its members suspect government trolls may have been responsible.

Blocking and Filtering

There have been no reported incidents of government efforts to block or filter internet content since April 2011, when the national regulator issued a directive to ISPs to temporarily block citizens’ access to Facebook and Twitter in response to the “walk to work” protests over rising food and fuel prices. According to news reports, most ISPs did not comply with the directive. Online content remains uncensored in Uganda as of 2015, and social media and blogging platforms are freely available.

Nevertheless, with the growing popularity of social media and communications applications for critical commentary, the government has periodically indicated intentions to block certain web platforms. Most recently in 2015, the government issued threats to shut down social media tools such as WhatsApp and Facebook in response to social media debates over the issue of revenge pornography and other forms of “computer misuse.”

Content Removal

To date, there have been no known instances of takedown notices issued for the removal of online content and no problematic issues of intermediary liability for service or content providers. In January 2015, however, the popular “Ugandans At Heart” Facebook page known for its political activism and criticisms of the government was taken down for allegedly breaching Facebook’s terms of service. The “Ugandans At Heart” administrator suspected the government’s hand behind the takedown, which would have required a coordinated effort by progovernment users to report the Facebook page as abusive. While denying involvement, anonymous government officials reportedly de-

---

scribed the takedown as “good news.” The page was eventually restored. Later in April, the group's Google forum was shut down after being flagged for “containing spam, malware, or other malicious content,” which forum moderators believe may also have been due to government interference.

Meanwhile, the Anti-Pornography Law enacted in February 2014 threatens to hold service providers criminally liable for uploading or downloading vaguely defined pornographic material on their systems, with penalties of up to five years in prison and fines of US$4,000. The law also establishes a Pornography Control Committee tasked with developing blocking software, which, once procured, service providers must install to preemptively filter and block “pornographic” content. Increasing government interest in curbing pornography and prostitution in the past year could further place intermediaries in a tough position over content hosted on their networks.

## Media, Diversity, and Content Manipulation

Content available online in Uganda is somewhat diverse, though news websites provided by the Vision Group, a media company that is partly owned by the government, are only available in four local languages (out of 40 languages and 56 native dialects). Newspapers such as Bukedde, Etop, Rupiny and Orumuri have created online platforms. Other news sites of major privately owned newspapers are only accessible in English, which is not widely spoken across Uganda. The Google Uganda domain is available in five local languages, while the Firefox web browser can be accessed in two languages, Luganda and Acholi.

Blogging continues to be popular among young Ugandans who have boldly taken to the internet to push the boundaries on controversial issues such as good governance and corruption.

Routine crackdowns and threats from the government—such as shutting down media houses perceived to be too critical of the government and reported police attacks on journalists—have engendered a culture of self-censorship among journalists both off and online. Taboo topics include the military, the president's family, the oil sector, land-grabs, and presidential terms. Nonetheless, critical commentary and opposition voices have become more vibrant online in recent years.

## Digital Activism

Internet use is steadily enhancing citizen participation in democratic processes as well as increasing

---


public scrutiny of government actions. Crowdsourcing and crowd-mapping tools have given citizens the ability to monitor elections, and a number of civil society groups are increasingly using SMS platforms and social media for advocacy and to call for protests. Nevertheless, digital media activism did not result in any largescale social or political change in Uganda during the coverage period.

Violations of User Rights

The number of individuals arrested for their online activities in Uganda increased in 2014-2015, compared to the previous coverage period. Government efforts to draft a Data Protection and Privacy Bill were initially seen as a positive step towards promoting the right to privacy, though the bill was later criticized for its overly broad and vague conditions in which personal data may be collected. Intimidation, threats of violence, and technical attacks against vulnerable groups and marginalized communities, particularly the LGBTI community, remained a growing concern.

Legal Environment

The Ugandan Constitution provides for freedom of expression and speech, in addition to the right to access information. However, several laws—including the Press and Journalist Act, sections of the penal code, and the Anti-Terrorism Act—appear to negate these constitutional guarantees for freedom of expression. For example, the Press and Journalist Act of 2000 requires journalists to register with the statutory Media Council, whose independence is believed to be compromised by the government’s influence over its composition. The penal code contains provisions on criminal libel and the promotion of sectarianism, imposing penalties that entail lengthy jail terms. While none of these laws contain specific provisions on online modes of expression, they could arguably be invoked for digital communications and generally create a “chilling effect” on freedom of expression both online and offline.

Meanwhile, the 2002 Anti-Terrorism Act criminalizes the publication and dissemination of content that promotes terrorism, vaguely defined, and convictions can carry the death sentence. Amendments to the act were passed by parliament in June 2015 and are currently awaiting the president’s signature. These proposed updates to the antiterrorism law include broadly defined provisions criminalizing the “indirect” involvement in terrorist activists and the “unlawful possession of materials for promoting terrorism, such as audio or video tapes or written or electronic literature.”

The 2011 Computer Misuse Act includes provisions that can specifically limit freedom of expression online. Under Act 2 of the law, the dissemination of “offensive communication” is prohibited alongside child pornography and cyber harassment, and is vaguely defined as the use of “electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person.” Offenses under this provision of the Act are considered misdemeanors and subject to fines, imprisonment of up to one year, or both.

Persistent government efforts to criminalize homosexuality in Uganda further threaten to restrict internet freedom. The now nullified Anti-Homosexuality Act enacted in February 2014 prescribed up to life imprisonment for committing the “offense of homosexuality,” putting the lives of countless...

Uganda

Ugandan LGBTI individuals at risk of discrimination, persecution, and violence. Pertinent to internet freedom, Article 13 of the law criminalizes the use of electronic devices—including “internet, films, and mobile phones—for the purposes of homosexuality or promoting homosexuality.” A person or entity convicted under this offence could be subject to a fine of UGX 100 million (approximately US$40,000), imprisonment of five to seven years, or both. A judicial ruling struck down the law in August 2014 based on an administrative technicality, which enabled the law’s ardent advocates to reintroduce the law in November 2014, though as of mid-2015, it is unclear when it would be presented to Parliament for adoption.

The Ugandan judiciary has been known to uphold press freedom and freedom of expression. In 2004, for example, the Supreme Court struck down a provision in the penal code criminalized the publication of false news, and in 2010, the Constitutional Court quashed the law on sedition.

Prosecutions and Detentions for Online Activities

The number of individuals arrested for their online activities in Uganda increased in 2014-2015, compared to the previous coverage period when no arrests or prosecutions were reported. In November 2014, three activists in western Uganda were arrested for allegedly inciting violence with posts written in the Facebook group the Masindi News Network (MANET), which disseminates information about the western region of the country to over 16,000 members and often posts demands for political accountability from the government. The Facebook group had recently sought to collect one million signatures for a petition urging Parliament to investigate the alleged mismanagement of funds for the construction of a major road in the region. The three activists were released three days later in response to the demands of hundreds of people who demonstrated in front of the police station, though their case is still being investigated as of mid-2015.

In February 2015, a man named Robert Shaka was summoned by police and subsequently arrested on suspicions of running the popular Facebook account called Tom Voltaire Okwalinga (TVO), which is well known for its politically charged posts that often accuse the Ugandan president and other senior leaders of corruption and incompetence. While in detention, the police searched Shaka’s home without a search warrant and confiscated some of his electronic devices. He was released on bond shortly thereafter but arrested again in June 2015 on charges of disseminating “offensive communication” under the 2011 Computer Misuse Act, charges Shaka denied. Shaka was later released on bail and awaits trial as of mid-2015.

Meanwhile, in May 2015, President Yoweri Museveni called for the arrest of three individuals whose

voices were heard in an audio clip disseminated widely via WhatsApp that reportedly contained abusive and sectarian language. According to observers, the government’s increased crackdown on online speech, particularly on social media platforms, in the past year may be an indication of restrictions to come in the lead up to the presidential election in 2016.

In 2014, the Uganda Police Force established a Cyber Crimes Unit to fight malicious technical attacks but was criticized by observers as an effort to intimidate users and encourage self-censorship “given the shifting trends from the use of traditional media to online.” According to research by Unwanted Witness Uganda, the unit has profiled ‘dozens of internet users particularly those deemed to be opponents of the government’ which is a worrisome trend as the country gears up for general elections in 2016. In mid-2015, the Cyber Crimes Unit publicly stated its mandate includes “threats that could destabilize the country” committed on social media platforms.

Surveillance, Privacy, and Anonymity

There is strong sense that government surveillance of citizens’ communications has heightened in recent years, particularly in response to increasing government activity to address the threat of terrorism in the region. In July 2015, email leaks from the Italian surveillance firm Hacking Team revealed that the Ugandan government began talks in April 2015 with the company to purchase its sophisticated spyware known as Remote Control System (RCS). While the leaked emails did not confirm the sale, they point to the government’s intent to acquire such technologies that can monitor and intercept user communications.

The government expanded its surveillance powers with the hurried passage of the 2010 Regulation of Interception of Communication (RIC) Act following the July 2010 Al-Shabaab terrorist attack in Kampala. Under the RIC, telecommunication companies are required to install equipment that enables real-time electronic surveillance of suspected terrorists. The RIC Act also gives the government permission to tap into personal communications for national security concerns, which can be requested by the security minister and granted after an order by a High Court judge. Service providers are further required to disclose the personal information of individuals suspected of terrorism to the authorities upon issuance of a court warrant or notice from the security minister on matters

55 Lawful interception is granted after issuance of a warrant by a judge if “there is an actual threat to national security or to any national economic interest, a potential threat to public safety, national security or any national economic interest, or if there is a threat to the national interest involving the State’s international relations or obligations.” See, Regulation of Interception of Communications Act, 2010 Section 5, September 3, 2010, http://bit.ly/1jQAVyP.
related to national security, national economic interests, and public safety. Failure to comply with the provisions in the RIC Act can entail penalties of up to five years in prison for intermediaries, in addition to license revocations. While it is not clear the extent to which the 2010 RIC Act has been implemented or operationalized, in March 2014, the government requested a supplementary budget of UGX 200 billion (over US$80 million) through 2019 to procure surveillance equipment and establish a monitoring center in accordance with the RIC Act.

In addition to the RIC Act, clauses in the 2002 Anti-Terrorism Act give security officers, appointed by the interior minister, the power to intercept communications of individuals suspected of terrorism and to keep them under surveillance, without judicial oversight.

Telephone companies reportedly “face undue influence and pressure from [the] government demanding for print-outs of phone calls made by any citizen without court orders... [which] have been used against activists or human rights defenders to justify their arrests, arbitrary detention or at times used as evidence in courts of law.” Nonetheless, telecom industry observers have noted that vibrant competition between service providers makes them reluctant to hand over information to the government without going through legal channels. However, observers do not rule out the possibility that some companies may cooperate quietly with government requests.

Anonymous communication is compromised by mandatory registration for mobile phone SIM cards and mobile internet subscriptions. Launched in March 2012, the process requires subscribers to provide a passport photo and ID, both residence and workplace addresses, and next of kin, among other personal details. Civil society groups cited concerns that “the mandatory SIM card registration was carried out to enable the use of surveillance equipment purchased and installed by telecom companies.”

In response to growing concerns over infringements on users’ right to privacy in Uganda, civil society pushed for data protection legislation in 2014, which led to the drafting of the Data Protection and Privacy Bill by year’s end. While the bill was initially well received, it was later criticized for being open to misinterpretation due to the broad and vague conditions in which personal data may be collected, such as for “national security” reasons. As of March 2015, reports emerged that the government lacks the funds needed to enact the data protection law, leaving user data without safeguards from unnecessary intrusion.

---

56 The Regulation of Interception of Communications Act, 2010, Section 8.
57 The Regulation of Interception of Communications Act, 2010, Section 62.
60 Unwanted Witness Uganda, The Internet: They Are Coming For It Too, January 17, 2014, 39, http://bit.ly/1FTb1rH. These allegations were denied by the security minister, who claimed that any phone tapping is done in compliance with the law, upon issuance of a court order, and for a limited period against users suspected of “subversive activities” and criminal activity. See: Deo Walusimbi, “Muruli Mukasa: I replace Sejusa,” The Observer, March 5, 2014, http://bit.ly/1kkKQUB.
61 Freedom House interviews.
62 Unwanted Witness Uganda, The Internet: They Are Coming For It Too.
63 Unwanted Witness Uganda, The Internet: They Are Coming For It Too.
67 Unwanted Witness, “Uganda government is lacking funds to enact a law on Data Protection and Privacy,” March 13, 2015,
Uganda

Intimidation and Violence

While print journalists have long faced a high degree of harassment and occasional violence for their reporting, these types of violations have begun to seep into the online sphere as well.

LGBTI activists, in particular, have reported increasing harassment, both offline and online, in recent years, with hate messages often pervading targets’ Facebook walls. In July 2014, Magembe Norma, an individual who created a petition on Change.org for the prosecution of Uganda’s top three leaders behind the anti-homosexuality movement in the country, reported that his life was in danger as a result of his online petition and activism. Also, increased cases of revenge pornography against female celebrities were reported in 2014-2015.

Technical Attacks

In addition to intimidation and threats of violence, technical attacks against vulnerable groups and marginalized communities remained a growing concern in Uganda in 2014-2015. According to an LGBTI individual in Uganda, a Ugandan gay rights activist had his Yahoo email taken over by unknown person(s) and all of his emails forwarded to a local mail host in 2014, though he was able to contact Yahoo and regain control over his email. Cases of blackmail were also reported, involving threats to expose the identities of several LGBTI individuals due to their perceived or real sexual orientation. In some cases, the blackmailers requested for money in exchange for their silence.

In addition, there were numerous reports of spyware and phishing attacks against several LGBTI individuals who received a large number of suspicious emails from familiar contacts. In another incident, one gay rights organization was hacked and defaced by unknown persons.

http://bit.ly/1CIYeRR


71 Robert Mugabe (2014)

Ukraine

Key Developments: June 2014 – May 2015

- Pressure from militants in eastern Ukraine resulted in temporary blocking of pro-Ukrainian content on servers hosted in the region (see Blocking and Filtering).

- In April 2015, 30,000 websites were temporarily shut down when Ukraine State Security Services seized servers from a data center believed to be hosting “anti-Ukrainian” content. Most of the websites were restored within a few weeks, though some remained offline (see Content Removal).

- The arrest of a journalist charged with treason for posting a video denouncing mandatory conscription signaled the Ukrainian government’s growing intolerance for critical content online (see Prosecutions and Detentions for Online Activities).

- Online journalists, activists, and bloggers in eastern Ukraine were subject to extralegal intimidation and were beaten, tortured, kidnapped, or otherwise assaulted during the period for their alleged pro-Ukrainian views (see Intimidation and Violence).

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>Partly Free</td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>17</td>
<td>19</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>33</td>
<td>37</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 42.9 million

Internet Penetration 2014: 43 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2015 Status: Partly Free
Editor’s Note

On March 16, 2014, a referendum held in Crimea resulted in Russia’s annexation of the territory from Ukraine. On March 27, the General Assembly of the United Nations issued a non-binding resolution calling the referendum invalid and urging member states and international organizations not to recognize any such change in Crimea’s status.

Freedom on the Net focuses on internet freedom developments as they pertain to internet users within each of the 65 countries under study. This report focuses primarily on the overall status of internet freedom in Ukraine from June 2014 through May 2015. Due to the ongoing crises in the region, events in Crimea during this time may be excluded from this report.

Introduction

The ongoing confrontation with Russia and the conflict in eastern Ukraine has led to an increase in censorship attempts on both sides in a bid to gain control over the information sphere. The tumultuous end of the Euromaidan protests in early 2014 was followed by Russia’s annexation of Crimea and the start of the prolonged conflict in eastern Ukraine. This period was characterized by a continued increase in civic activity online and the widespread use of social networks for grassroots volunteer organizing, as well as coordinating information flows and fighting the information war with Russian and pro-Russian forces.

The internet is fast becoming a major field in an information war with Russia, with activists and journalists cooperating to debunk Russian propaganda and verify key facts about the events in Ukraine for the rest of the world. Online discussion forums and social media were significantly impacted by partisan voices, paid mass commenting, and other manipulation attempts coming from Russia. The separatist uprisings supported by Russian forces in the Donetsk and Luhansk regions of eastern Ukraine led to further efforts on both the pro-Russian, separatist side and the Ukrainian side to crack down on undesirable content, including online, encouraging an atmosphere of fear and self-censorship, especially in occupied regions.

The security of journalists and online users further deteriorated during the conflict in eastern Ukraine, where reporters, activists and bloggers faced extreme intimidation and physical violence as they were explicitly targeted for their work by Russian-backed militants. Additionally, independent online media and civic initiatives in eastern Ukraine faced multiple cyberattacks during the period. At the same time, Ukrainian officials and law enforcement targeted separatist websites and “extremist” content on social media in an attempt to restore control over the online information sphere.

Economic troubles in the country and the upheaval in eastern Ukraine contributed to a slump in the telecommunications market. Although internet penetration continued to grow, the contestation of control over communications in eastern Ukraine has created new obstacles to internet and mobile access for parts of the country.

Online media outlets and social media platforms continue to play an important role as Ukraine faces new challenges, with activists using them for organizing and promoting ideas such as coordinating volunteer support for the military, aid efforts to internally displaced populations, government oversight, and corruption investigations of former (or current) officials. Government officials and civil servants continue to be more active online, and are becoming savvier in using the tools to indicate accountability in their everyday work.
Obstacles to Access

Ukraine’s telecommunications market has suffered during the reported period due to economic hardships in the country and the crisis caused by Russia’s annexation of Crimea and later, the upheaval in eastern Ukraine. Although internet penetration continues to grow, other obstacles to access, such as damage to infrastructure in the eastern region, have obstructed internet and mobile access for parts of the country.

Availability and Ease of Access

Internet penetration in Ukraine continues to grow steadily, due in part to diminishing costs and the increasing ease of access, particularly to mobile internet. According to the International Telecommunication Union (ITU), Ukraine had an internet penetration rate of 43 percent in 2014, compared to 41 percent in 2013 and just 18 percent in 2009. At the same time, 2015 statistics from Pew Research Center show that of all Ukrainian adults, 53 percent access the internet at least occasionally or own a smartphone. Pew Research Center also found that 73 percent of Ukrainian adults who do have access to the internet use it on a daily basis. For fixed-line broadband subscriptions, the penetration rate was approximately 8.8 percent at the end of 2013, while mobile broadband had a penetration rate of just over 5 percent. Meanwhile, according to Akamai, the average broadband connection speed in Ukraine was 9.3 Mbps in the fourth quarter of 2014 (compared to 7.3 Mbps in the third quarter of 2013), and access to broadband internet in Ukraine is fairly affordable. A monthly unlimited data plan with a 1 Mbps broadband channel costs UAH 80–120 (US$3.80–5.70), while the average monthly wage in the country was UAH 3,998 (US$190) in April 2015.

Among current internet users, 82 percent live in urban areas, 37 percent of whom live in cities with a population over 500,000. However, internet penetration in rural areas has also been growing and is currently about 18 percent. The level of infrastructure differs between urban and rural areas, contributing to the urban-rural divide. Most people access the internet from home or work, though many middle- and higher-end cafes and restaurants also provide free Wi-Fi. Access is also common in public libraries and schools. Internet cafes still exist but are gradually losing popularity.

Mobile phone penetration has plateaued, hovering around 131 percent in 2014. Use of mobile

---

internet is gaining in popularity, and an estimated 31 percent of Ukrainian mobile subscribers own smartphones.\(^\text{11}\) Cost continues to be the main barrier to higher mobile internet use. In February 2015, mobile operators finally gained access to the military’s share of third-generation (3G) mobile phone frequencies, with the three major mobile providers all acquiring licenses for providing 3G services.\(^\text{12}\) All three companies started commercial exploitation of the frequencies in the summer of 2015 and 3G mobile internet access is currently priced at 100-150 UAH ($4.50-7) for 2-3 GB of traffic per month.\(^\text{13}\)

**Restrictions on Connectivity**

In late spring and summer of 2014, Russian and pro-Russian forces occupied the Crimean peninsula, and later took control of parts of the Donetsk and Luhansk regions. Along with political control, those forces also attempted to disrupt or regulate access to telecommunications. While some disruptions in internet and mobile connectivity were caused by military activity, especially in eastern Ukraine (e.g., cell towers or internet cables damaged by explosions),\(^\text{14}\) in some cases there was direct pressure on ISPs from rebel militias and Russian-supported authorities, causing them to take offline or block particular services, such as city web cameras in Luhansk,\(^\text{15}\) or Ukrainian news websites in Donetsk\(^\text{16}\) and Crimea\(^\text{17}\) (see Limits on Content). In February 2015, armed men attacked the office of telecom provider Ukrtelecom in Simferopol, Crimea, and disconnected communication lines between Crimea and mainland Ukraine.\(^\text{18}\) As of May 2015, none of the Ukrainian mobile providers are operating in Crimea.\(^\text{19}\)

The backbone connection of UA-IX (Ukrainian internet exchange, a mechanism of traffic exchange and connection to the wider internet for Ukrainian ISPs) to the international internet is not centralized, and major ISPs each manage their own channels independently. Ukraine’s internet infrastructure is diverse, with more than 200 domestic autonomous systems purchasing direct international transit service (out of a total of more than 1,650 domestic autonomous system numbers). The country has a well-developed set of at least eight regional internet exchanges, as well as direct connections over diverse physical paths to the major Western European exchanges.\(^\text{20}\)

---

\(^{11}\) Ibid.
\(^{19}\) Vadym Karpus, ““Интертелеком” уйдёт из Крыма с 1 мая,” [“Intertelecom” to leave Crimea starting on May 1] ICTua, April 15, 2015, http://bit.ly/1P7x4Ql.
ICT Market

The Ukrainian telecommunications market is fairly liberal and is currently undergoing gradual development. The state previously owned 93 percent of the largest telecom company and top-tier ISP, Ukrtelecom, but the company was privatized in March 2011.\(^{21}\) Though no longer state-owned, Ukrtelecom is still the largest ISP in the country and possesses Ukraine's primary network, trunk, and zone telecom lines.\(^{22}\) Other telecommunications providers are dependent on leased lines, since Ukrtelecom owns the majority of the infrastructure, and many alternative providers do not have sufficient resources to build their own networks. However, Ukrtelecom does not exert any pressure or regulatory control over other ISPs.

Among the major private ISPs in Ukraine are Volia, Triolan, Vega, and Datagroup; however, major mobile service providers, like Kyivstar and MTS, also provide broadband internet access.\(^{23}\) There are about 400 ISPs in Ukraine, according to the National Commission for the State Regulation of Communications and Informatization (NCCIR).\(^{24}\) Regional ISPs are usually smaller local businesses, and regional dominance largely depends on business and other connections in a specific region, making the market prone to corruption.

Ukrchastotnagliad, the Ukrainian frequencies supervisory center, reports that 86 operators have licenses to provide satellite communication services in Ukraine. Companies providing internet access using satellite technologies in Ukraine include Ukrsat, Infocom-SK, Spacegate, Adamant, LuckyNet, Ukrnet, and Itelsat. With the exception of Infocom-SK,\(^{25}\) all of these companies are privately owned.\(^{26}\) The three major players in the mobile communications market are Kyivstar (owned by Dutch VimpelCom Ltd.), MTS Ukraine (owned by Russian AFK Sistema), and “life:)” (owned by Astelit, whose main shareholders are the Turkish company Turkcell and Ukrainian System Capital Management). Together, these companies hold 94.6 percent of the mobile communications market.\(^{27}\)

There are no obvious restrictions or barriers to entry into the ICT market, but any new business venture, whether an ISP or an internet cafe, faces obstacles including bureaucracy and corruption, as well as the legal and tax hurdles common to the Ukrainian business environment. In particular, the Ukrainian ICT market has been criticized for its difficult licensing procedures for operators, and under the 2003 Law on Communications, operators are required to have a license before beginning their activities.

Regulatory Bodies

The ICT sector is regulated by the National Commission for the State Regulation of Communications

---


\(^{24}\) “Во 2 квартале количество абонентов провайдеров Интернет увеличилось на 6.4%,” [In Second Quarter Number Of Subscribers Of Internet Providers Grew By 6.4%] Delo, July 26, 2007, http://bit.ly/1BA2elL.


\(^{26}\) OpenNet Initiative, “Ukraine.”

Ukraine

and Informatization (NCCIR). Members of the NCCIR are appointed by the president of Ukraine. Due to widespread corruption in the political system and the lucrative nature of business in the ICT sector, appointments to the commission have lacked transparency. The NCCIR’s work has often been obstructed by claims of non-transparent decisions and operations. Furthermore, the 2003 Law on Communications does not guarantee the independence of the NCCIR. However, the newly appointed head of the NCCIR has vowed to reform the regulator in 2015, and is working on a bill that will guarantee both the financial independence of the NCCIR and its independence from the executive branch of state power.29

A parliamentary committee on informatization and information technologies was created in December 2012,30 ostensibly to promote the president’s promise of further development of the Ukrainian ICT market.31 So far, the committee has not made any significant decisions relating to the ICT industry.

A new Ministry of information Policy was created in December 2014,32 to promote information security and regulate information policy, including online. Although the concrete regulatory powers of the new ministry remain unclear, media advocates and journalists have branded the department, aimed at protecting Ukraine in the information war with Russia, “Orwellian,”33 and have expressed concern that the agency will only hinder freedom of speech and set a dangerous precedent, granting the new government a greater measure of control over Ukrainian media.

Limits on Content

The Russian annexation of Crimea in March 2014 led to an all-out information war, with Russian and Ukrainian TV channels taken off the air in mainland Ukraine and Crimea, respectively. Access to online content remained largely unaffected by these events, although online discussion forums and social media were significantly impacted by partisan voices, Russian-paid commenting, and self-censorship out of fear. The separatist uprisings supported by Russian forces in Donetsk and Luhansk regions of eastern Ukraine led to further efforts on both the pro-Russian and the Ukrainian sides to censor undesirable content, including online.

Blocking and Filtering

There are no permanent blocks, filtering mechanisms, or blacklists for online websites in Ukraine. YouTube, Facebook, Twitter, and blog-hosting services such as Wordpress and LiveJournal are freely available and gained significantly more users since the Euromaidan protests in 2013-2014.34 Since

34 Olga Minchenko, “Близько 6 млн українців в січні хоча б 1 раз відвідували Facebook та 11 млн – ВКонтакте,” [About 6
Ukraine

the start of the crisis in eastern Ukraine, Ukrainian authorities have attempted to put pressure on ISPs to introduce selective blocking of websites containing “separatist” or “terrorist” content, but the ISPs have refused wholesale blocking, and insist court orders must be provided in each case in order for a website to be blocked or taken down. Individual accounts of social media users containing calls to “separatism” or “extremism” have also been targeted (see Prosecutions and Detentions for Online Activities).

Russian-backed separatist militants in eastern Ukraine have been more proactive in blocking Ukrainian resources, cracking down on Ukrainian news websites in Donetsk. In September 2014, ISPs in Donetsk received letters from “officials” in the region demanding that they block 27 Ukrainian news websites—at least some complied, as internet users reported that they were unable to access some of the sites. In May 2015, the self-proclaimed “Donetsk People’s Republic” followed Russia’s example in instituting an official blacklist of websites banned on its territory, though the list is not public and it is unclear to what extent DPR officials would be able to enforce it.

Content Removal

In April 2015, in an attempt to block five allegedly anti-Ukrainian websites, the Ukrainian Security Service officers seized hosting servers at four data centers in Kyiv of the web-hosting company NIC.ua, also the largest domain registrar in Ukraine. As a result, 30,000 Ukrainian websites that had nothing to do with the targeted websites were also taken offline. It turned out that all but one of the five websites suspected of separatism only used NIC.ua as a registrar, and hosted their content on servers in Russia. The Security Service claimed that it had officially requested that NIC.ua block the targeted websites, but the company did not comply. NIC.ua denied the fact that they received any official requests and noted that it is illegal in Ukraine to block websites based on a scanned request or warrant, and that proper procedure would require original court documents. Within a few weeks, over 90 percent of the websites had been restored.

There is no current regulatory framework for systematic censorship of content online, although prior to the change in government in 2014, there were several attempts at creating legislation that could censor or limit content. Many of these initiatives presented indirect threats to freedom of information online. For example, in September 2012, members of parliament introduced a draft bill that suggested implementing jail sentences of three to five years for cybercrimes such as hacking, cyber-scams, and information espionage. Additionally, there were calls to create a national cybersecurity system as part of the strategic law “On the main foundations of development of information society in Ukraine for 2007–2015.” In some cases, such laws obligate ISPs to remove or block the offensive

40 National Commission on Communications and Informatization, “НКРЗІ пропонує зміни до Закону Україні “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки;” [NCCIR proposes changes to the Law of Ukraine
Ukraine

or illegal content within 24 hours or, if such content is found to be hosted outside of Ukraine, ISPs would have to limit Ukrainian users’ access to such content, effectively introducing a practice of filtering content.

Media, Diversity, and Content Manipulation

Amid the conflict in eastern Ukraine, online journalists, commentators and internet users have been pressured to self-censor, especially on topics directly related to the Russia-backed insurgency in the east, and the themes of separatism, terrorism and patriotism. Self-censorship has been more pronounced in the parts of eastern Ukraine occupied by pro-Russian forces and in Crimea, where internet users and journalists have faced attacks, abuse, and intimidation for their pro-Ukrainian positions. However, the media landscape remains varied, and different viewpoints are readily available to users online, especially on social media.

Journalists in Ukraine found themselves suddenly covering warfare, with limited access to occupied parts of Ukraine and unfamiliar and dangerous working conditions presenting a challenge. Online media outlets like Hromadske TV, Ukrainian Radio Svoboda, and Donbass News produced fearless photo and video coverage of military activity, civilian losses, and life in occupied territories, often relying on help from undercover reporters and social media users in eastern Ukraine. Several journalist initiatives were also set up after the Russian invasion of Crimea to battle Russian media propaganda and debunk the myths distributed by Russian media outlets.

Attempts to manipulate the online landscape have mostly been external and come from the Russian side in the form of mass commenting and paid posts on social media, as well as fake websites, and social media groups set up by pro-Russian internet users. The Ukrainian Ministry of Information has attempted to respond in kind to the organized Russian information manipulation efforts by creating its own “internet army,” but its actions have not seen much praise from Ukrainian internet users.

Digital Activism

The Ukrainian social media sphere expanded dramatically during the Euromaidan protests, with new groups and communities popping up and the use of Facebook and Twitter growing rapidly. By the end of 2014, Twitter use in Ukraine grew 56 percent, and Facebook use grew 9 percent, compared to the end of 2013.
Ukraine

With the annexation of Crimea and the start of the conflict in eastern Ukraine, activists and volunteers mobilized during Euromaidan48 found new uses for online platforms and their networks,49 switching their efforts over to help fundraise for the needs of the military and volunteer battalions, provide information and assistance to refugees, and help to those kidnapped by the pro-Russian militias or Crimean forces. Citizen journalists also used open-source tools and data to track the presence of Russian troops50 and military equipment in Ukraine.51 Many officials in the new Ukrainian government use Facebook and Twitter heavily to report on their actions, and regularly respond to comments and take into account public opinion in their work, helping to increase accountability.52

Violations of User Rights

The security of journalists and online users further deteriorated during the conflict in eastern Ukraine, where reporters, activists and bloggers faced extreme intimidation and physical violence as they were explicitly targeted by paramilitary groups for their work and views. Additionally, independent online media and civic initiatives in eastern Ukraine faced multiple cyberattacks during the period. At the same time, Ukrainian officials and law enforcement targeted separatist websites and “extremist” content on social media in an attempt to restore control over the online information sphere.

Legal Environment

The right to free speech is granted to all citizens of Ukraine under Article 34 of the constitution, although the article also specifies that the state may restrict this right in the interest of national security or public order. Part three of Article 15 of the constitution forbids state censorship. In practice, however, these rights have been frequently violated. Especially grave violations were observed in occupied parts of eastern Ukraine, where journalists and regular internet users faced attacks, kidnappings and extralegal intimidation for their reporting or pro-Ukrainian views. In addition, Article 171 of the criminal code provides fines and detention sentences for obstructing journalists’ activity, but in parts of eastern Ukraine controlled by Russian-backed militants, journalists were often unable to gain access or do reporting work.

There is no specific law mandating criminal penalties or civil liability for online and ICT activities, but other laws, such as those penalizing extremist activity, terrorism or calls to separatism (based on Article 100, part 1 of the Ukraine Criminal Code – threats to territorial integrity and sovereignty of Ukraine, punishable with three to five years in jail), also apply to online activity.

Prosecutions and Detentions for Online Activities

Ukrainian authorities have detained and prosecuted a number of online users and journalists on ac-
Ukraine

cusations of online extremist activity or related charges. In July 2014, a Dnipropetrovsk citizen was sentenced to three years in jail for “calls to separatism” after he created and promoted a page for “Ukrainian autonomous Republic” (as part of the Russian Federation) on a social media website.53

In February, Ukraine’s Security Service arrested journalist Ruslan Kotsaba on charges of treason after he posted a YouTube video calling viewers to boycott military mobilization in Ukraine.54 Kostaba’s arrest caused heated debates about the balance between information security and freedom of speech online during an armed conflict, and he remains in detention while his trial is ongoing.

In May 2015, Ukraine’s Security Service detained two internet users in eastern Ukraine who allegedly created and administered 26 groups on Vkontakte (a Russian social networking site) said to be “anti-Ukrainian.”55 The users were accused of “aiding terrorist activity” and are currently under investigation.

Surveillance, Privacy, and Anonymity

The pervasiveness of extralegal surveillance of Ukrainian users’ activities is unclear. A new proposal by the State Service on Special Communications and Information Security mandates that all mobile phone users, including those using prepaid packages, would have to register and disclose their personal data (such as their passport number) with mobile providers.56 The committee, which is working on the legal framework for the proposal, claims pressure from law enforcement to institute the measure, given the terrorist and security threats Ukraine currently faces. So far only a draft of the proposal has been published on the government website,57 but has caused widespread criticism from the industry and free speech advocates. There is currently no obligatory registration for either internet users or mobile phone subscribers.

From 2002 to 2006, mechanisms for internet monitoring were in place under the State Committee on Communications’ Order No. 122, which required ISPs to install so-called “black-box” monitoring systems that would provide access to state institutions. This was ostensibly done to monitor the unsanctioned transmission of state secrets. Caving to pressure from public protests and complaints raised by the Internet Association of Ukraine and the Ukrainian Helsinki Human Rights Union, the Ministry of Justice abolished this order in August 2006.

In December 2013 the NCCIR released a new edition of “Rules for Activities in the Sphere of Telecommunications,” which included a problematic paragraph about ISPs and telecom providers having to “install at their own cost in their telecommunications networks all technical means necessary for performing operative and investigative activities by institutions with powers to do so.”58 Some human rights groups and internet associations are concerned that this step will aid the Security Ser-

58 NCCI, Rules for Activities in the Sphere of Telecommunications.
services and the government in restricting internet freedoms by creating additional means of pressure that the government can exert over ISPs. 59

In June 2014, Russian-backed militants in the self-proclaimed “Donetsk People’s Republic” demanded that local ISPs hand over all data on their users, including logins, email addresses, contact lists, and account activity. 60 At least some of the ISPs reported that they were attempting to determine whether or not they had to comply, and there is no confirmed evidence to date that any of the ISPs turned over user data.

Intimidation and Violence

The conflict in eastern Ukraine brought a fresh wave of intimidation against online activists and journalists, with multiple reports of kidnappings, threats, and physical violence. 61 Activists, bloggers and regular internet users faced extreme intimidation and physical violence as they were explicitly targeted for their work or pro-Ukrainian views by Russian-backed militants. International journalists reporting on the conflict have also faced threats.

Sergey Sakadynsky, editor of Luhansk internet publication “Politika 2.0,” was kidnapped by pro-Russian militants in early August 2014 together with his wife, accused of being “a Euromaidan activist,” and spent months in captivity. Sakadynsky was only released in January 2015. Many other eastern Ukrainian journalists and bloggers have spent at least a few weeks “in the cellars,” and have usually been accused of aiding the Ukrainian side or publishing pro-Ukrainian content online. 62

In April 2015, militants from self-proclaimed “Donetsk People’s Republic” attacked a freelance reporter working for online media outlet Hromadske TV Donbas, 63 destroying his apartment and taking his hard drive.

Later in April, a local journalist in Kakhovka, southern Ukraine, faced intimidation from representatives of the militarized right-wing volunteer group “Pravy Sector” over a Facebook post in which she suggested that civic activist groups shouldn’t wear camouflage. 64 The reporter was accosted by the group members after a local government session, and says they tried to use force on her, but she was rescued by local MPs.

Luhansk online journalist and activist Maria Varfolomeeva has been detained by separatists since January 2015, and has been accused of aiding the Ukrainian army. 65 Pro-Kremlin media outlet LifeNews recently released a video of the captive woman, where she begs to be released.

---

59 Oleg Shynkarenko, Зашморг на інтернет [A Noose on the Internet], INSIDER, January 8, 2014, http://www.theinsider.ua/business/52bac42dd8f4d/
Technical Attacks

Cyberattacks became a more common tactic in Ukraine after the annexation of Crimea and during the conflict in eastern Ukraine, with both pro-Ukrainian and pro-Russian sites attacked and individual users hacked. Hacker collectives like the pro-Russian “Cyber-Berkut,”66 and the pro-Ukrainian “Ukrainian Cyber Forces,”67 were active in penetrating websites, leaking documents, hijacking printers and web cameras,68 and blocking online payment accounts.69

In June 2014, a Donetsk regional journalist union found their website hijacked by “Donetsk People’s Republic” activists.70 Having gained full control of the website, the pro-Russian separatists used it to publish their own announcements.

In February 2015, Ukrainian soldiers serving in the “anti-terrorist operation” zone in eastern Ukraine found their mobile phones flooded with provocative messages from unknown numbers. The messages said “We’ve been betrayed;” “All is lost;” “It’s time to run;” and other demoralizing sentiments.71 The mass messaging likely involved special equipment, used to discover mobile signals in a geo-located area, intercept numbers and send mass texts.

In May 2015, Ukrainian TV channel STB reported that hackers had taken control of their YouTube channel, deleted all the videos, and published a “propagandist pro-Russian video” about the conflict in Ukraine on the page instead.72

---

United Arab Emirates

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>31</td>
<td>32</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>67</td>
<td>68</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

| Population:                           | 9.4 million |
| Internet Penetration 2014:            | 90 percent  |
| Social Media/ICT Apps Blocked:       | Yes         |
| Political/Social Content Blocked:    | Yes         |
| Bloggers/ICT Users Arrested:         | Yes         |
| Press Freedom 2015 Status:           | Not Free    |

Key Developments: June 2014 – May 2015

- The website of the Beirut-based Gulf Center for Human Rights, a nongovernmental organization, was blocked in January 2015 (see Blocking and Filtering).

- In August 2014, the president issued a new antiterrorism law containing overly broad definitions of terrorism—including undermining national unity, possessing materials counter to the state’s notion of Islam, and "publicly declaring one’s animosity or lack of allegiance to the state or the regime" (see Legal Environment).

- Nasser al-Faresi and Osama al-Najjar were each sentenced to three years in prison for criticizing the judiciary’s handling of the “UAE 94” trials against political dissidents. Several others were imprisoned for nonviolent speech that was critical of state institutions (see Prosecutions and Detentions for Online Activities).

- In October 2014, details emerged over the arrest and subsequent deportation of Iyad el-Baghdadi—a Palestinian blogger, longtime UAE resident, and vocal human rights advocate—to Malaysia. A critic of both secular and Islamist political forces, el-Baghdadi was not formally charged with any crime and lacked the necessary travel papers to enter Malaysia, where he spent several weeks in detention (see Prosecutions and Detentions for Online Activities).

- In February 2015, Omani blogger Muawiyah Alrawahi was arrested while crossing the UAE border and, as of publication, remained in detention on charges of insulting the country and its rulers via Twitter. Three sisters also disappeared for three months following tweets in support of their imprisoned brother (see Intimidation and Violence).
United Arab Emirates

Introduction

The United Arab Emirates (UAE) maintains an authoritarian grip on both politics and telecommunications. The country’s two mobile phone and internet service providers are either directly or indirectly owned by the state, reflecting a lack of checks and balances when it comes to surveillance and government requests to companies to hand over their customers’ personal data. Ongoing crackdowns on users have increased self-censorship on social media and online news outlets, of which the most prominent are government-owned. Numerous websites are blocked and search results are filtered in order to prevent access to local and international voices that differ from the state line, particularly on political, religious, and sexual matters. Current legal restraints, coupled with a judiciary that fundamentally lacks independence, create a highly problematic legal environment where users cannot be guaranteed that their constitutional and internationally recognized rights will be upheld.

A new antiterrorism law was issued in August 2014, providing lengthy prison sentences for crimes such as undermining national unity, possessing materials counter to the state’s notion of Islam, and “publicly declaring one’s animosity or lack of allegiance to the state or the regime.” The country’s 2012 cybercrime law already contains punishments for offending the state, its rulers, and its symbols, or for insulting Islam and other religions. As such, nonviolent opposition activists are often targeted under laws designed to counter terrorists and cybercriminals. At least five users are serving seven to ten-year sentences for their online activities as part of the so-called “UAE94” trials targeting 94 alleged members and supporters of the banned political opposition group, al-Islah. Six social media users have since been sentenced to three to five years for criticizing the judicial process or calling attention to human rights abuses, often regarding their jailed family members. For instance, Osama al-Najjar was sentenced to three years in September 2014 for alleging that his father was tortured while in prison. Foreign nationals are also targeted under harsh laws regulating social media use, resulting in their arrest and often deportation.

The government has embraced information and communications technology (ICT) as a means of developing a competitive economy and improving citizen services. Indeed, the UAE is ranked 23rd in the World Economic Forum’s 2015 Networked Readiness Index.1 While remaining open to receiving large amounts of foreign investment and expatriate workers, the government has actively fought to deter political discussions, demands for reforms, and criticism of public officials online. The first reported instance of law enforcement bodies targeting ICT use for political motives occurred in July 2010, when an 18-year-old named Badr al-Dhohri was held in Abu Dhabi for using his Blackberry to pass along a message that called for a protest against increases to the price of gasoline.2 Between 2011 and 2015, dozens have been detained for their political discussions on online forums and social media. Many have reported that they were held without charge, denied the right to an attorney, and in some cases, tortured.

---

Obstacles to Access

Similarly to other Gulf States, Emirati users enjoy a robust information and communications technology (ICT) infrastructure and high connection speeds. The ITU’s Measuring the Information Society (MIS) 2014 report ranked the UAE 32nd in the world. Similarly, the UAE is ranked 23rd in the World Economic Forum’s 2015 Networked Readiness Index. However, market conditions are not free, with top telecoms fully or partially owned by state entities.

Availability and Ease of Access

While the use of broadband is widespread, prices are extraordinarily high; the UAE has one of the most expensive broadband rates in the world, with high-end subscriptions costing more than AED 8,000 (US$2,178) a year. However, the UAE ranks 22nd in the ITU’s 2014 ICT Price Basket Index, in which local broadband prices are measured against, gross national income (GNI) per capita. This reflects a sense that despite the high prices, the internet remains affordable for most Emiratis, though not necessarily to all migrant workers.

The number of internet users has risen rapidly from a penetration rate of 61 percent in 2007 to 90.4 percent in 2014 according to the Telecommunications Regulatory Authority (TRA). The expansion of wireless broadband penetration has doubled from 45 percent (in 2012) to 90 percent (in 2013). As of February 2015, there were 1,145,216 internet subscribers in the country, 99 percent of whom had broadband connections.

The UAE has one of the highest mobile phone penetration rates in the region at nearly 178 percent representing 16.8 million subscriptions in 2014. In 2014, the Emirates ranked first in smartphone penetration in the Middle East region with 60.9 percent of total users.

Etisalat upgraded broadband speed twice, once in September 2014 and again in April 2015 for 100,000 business clients. In March 2015, Etisalat signed a partnership with Ericsson at the Mobile World Congress in Barcelona to implement 5G technology making the UAE the first in the region to take this step.

According to UNICEF, literacy in the Emirates was reported at 94 percent among males and 97 per-
United Arab Emirates

cent among females, and thus does not constitute a strong obstacle to internet use.\textsuperscript{13} UAE schools are now among the top 25 worldwide for online connectivity. There are now 123 smart-learning schools, compared with only 14 in 2012. The program benefits 11,402 students, who are also equipped with tablets. The ministry has also completed the e-content project in both English and Arabic. Principals are enrolled in international computer literacy training programs.\textsuperscript{14} By 2017, the country expects its Smart Learning Program to be installed in all K-12 government school classes; replacing textbooks with tablets and allowing students to interact with educators through an online platform.\textsuperscript{15}

Restrictions on Connectivity

In the Emirates, internet service providers (ISPs) are owned by the state. In 2008, Etisalat had announced the rollout of its nationwide fiber optic backbone. This May, Etisalat selected TeliaSonera International Carrier (TSIC) as its preferred global internet backbone provider under a framework deal.\textsuperscript{16}

The country’s two internet service providers—Etisalat and du—have launched their own carrier-neutral international internet exchange points, Smarthub and Datamena, respectively.\textsuperscript{17} Cuts to undersea cables have disrupted internet access for Emirati users on several occasions, though government-instituted outages are not known. In November 2013, du issued a statement that submarine cables were experiencing faults affecting their internet bandwidth.\textsuperscript{18} In March 2013, Etisalat warned that users would face slower speeds due to the cutting of a fiber-optic cable off of the Mediterranean coast of Egypt.\textsuperscript{19} Du suffered similar disruptions in April 2010 and March 2011 due to cuts to the SEA-ME-WE 4 cable.\textsuperscript{20} In 2008, 1.7 million users in the UAE were affected by undersea damage to submarine cables occurring at five separate locations around the globe.\textsuperscript{21}

ICT Market

Both Etisalat and du are, directly or indirectly, owned by the state. The UAE government maintains a 60 percent stake in Etisalat through its ownership in the Emirates Investment Company,\textsuperscript{22} while a majority of du is owned by various state companies.\textsuperscript{23} In June 2015, the government announced a decision to allow up to 20 percent of Etisalat shares to be held by foreign investors.\textsuperscript{24} The two companies are also the major mobile phone operators.

United Arab Emirates

Regulatory Bodies

Providers fall under the laws and regulations set by the Telecommunications Regulatory Authority (TRA). The authority was established in 2003 and is responsible for the management of “every aspect of the telecommunications and information technology industries in the UAE.” Its objectives include ensuring quality of service and adherence to terms of licenses by licensees, encouraging telecommunications and IT services within the UAE, resolving disputes between the licensed operators, establishing and implementing a regulatory and policy framework, and promoting new technologies.\(^\text{25}\)

In March 2015, the TRA and Dubai police launched the campaign “Digital Blackmail” calling on users to report incidents of cybercrime and blackmailing, which are punished with ten years in jail. An official from the Department of Cybercrime at Dubai Police said the police received 81 complaints in 2013 and registered 59 cases. The figure went up in 2014 with 212 complaints received and 73 cases registered.\(^\text{26}\)

In extension of its “My Number, My Identity” campaign launched back in June 2012, the TRA called on users to “reregister their SIM cards before documents expire” to avoid cancellations. The Authority said the move was “the result of studies that suggested an increase in civil and criminal cases related to the misuse of SIM cards.”\(^\text{27}\)

Limits on Content

*Online censorship has increased in the UAE following the Arab uprisings of 2011 as authorities blocked numerous websites and web forums where users openly call for political reforms or criticize the government. While self-censorship is pervasive, the ongoing crackdown against online dissent points to the fact that a limited number of users continue to use their real names when addressing sensitive issues. The families of political detainees use social media to highlight human rights abuses and communicate on behalf of their loved ones. The refusal of state-run news sites to cover controversial issues and trials has increased the importance of Twitter. These factors contribute to a highly controlled online environment in which freedom of expression and the right to information is not respected.*

Blocking and Filtering

The TRA instructs ISPs to block content related to terrorism, pornography, and gambling, as well as websites that contain political speech threatening to the ruling order. According to Herdict, the crowdsourcing tool that lets users report blocked content, internet users from the UAE have reported several social, political, LGBTQ, dating, and proxy sites blocked in their country.\(^\text{28}\)

In December 2014, a website run by anonymous employees of Emirates airlines was reported to be blocked in the country.\(^\text{29}\) The website of Beirut-based NGO Gulf Center for Human Rights was


\(^{27}\) "Re-register your SIM cards before documents expire," *Khaleej Times*, July 28, 2015, [http://yaho.it/1k6Zv7](http://yaho.it/1k6Zv7).


United Arab Emirates

blocked in January 2015. On Reddit, users reported the blocking of archive.today, a tool that keeps snapshots of URLs entered in case content disappears or gets modified. iHerb.com, an online retailer of nutritional supplement and wellness products, was reported to have been banned in June 2015.

The telecommunications company du details what criteria it used to block websites in a document available on its website. Prohibited content includes information related to circumvention tools, the promotion of criminal activities, the sale or promotion of illegal drugs, dating networks, pornography, homosexuality, gambling, phishing, spyware, unlicensed VoIP services, terrorism, and material that is offensive to religion.

No similar list was made available by Etisalat, although the company does have a space on its website where users can request that a website be blocked or unblocked. In 2005, an Etisalat spokesman stated that the company is not responsible for internet blocking and revealed that all complaints and requests are passed on to the Ministry of Information. He also claimed that a list of websites to be blocked is compiled by an American company and then implemented through a proxy server. Etisalat and du have responded to Twitter users about unblocking inquiries by asking them to fill certain online forms, yet there is no information on whether bans have been lifted in response.

The TRA, working with the Ministry of Communications, has also blocked five hundred search terms. An Emirati blogger tweeted that unblocking requests do not get responses from providers. Users have also reported blocked Twitter content such as political hashtags relating to local detainees. Blogger Ahmed Mansoor initiated a Twitter campaign using the hashtag #blocked_sites_in_uae to reveal which websites were blocked by the TRA. Most websites blocked were related to political dissent such as the Muslim Brotherhood or regional NGOs. According to the TRA, 82 percent of the websites blocked during the period from January to March 2015 were blocked for nudity and dating content, 8 percent for violating UAE laws, and 9 percent for containing phishing, hacking, and spyware content.

Skype's download page and online forum continued to be blocked during the coverage period, alongside several proxy websites. In May 2015, several users reported the storytelling platform Wattpad blocked in the UAE. Earlier in 2015, the dating app Tinder was blocked. A similar app,
United Arab Emirates

Jeltee, was launched by two Armenian expats and marketed as an app for forming friendships and connections rather than casual dating.44

The Lebanese queer and feminist e-magazine Bekhsoos45 and the U.S.-based Arab Lesbian e-magazine Bint El Nas are both blocked.46 Many websites displaying religious content are blocked, including an Arab-Christian online forum named The Church Network.47 A number of secular and atheist websites and forums in Arabic continue to be blocked such as 3almani.org, secularkuwait.freeforums.org, nadyelfikr.net, alawan.org, ladeenyon.net, and ladeeni.net.48

With the Emirates' support for the military coup in Egypt, the website Cairo Portal reported being blocked in the UAE, alongside other unnamed Egyptian websites, following their critical reports of the Gulf country's political stand.49 Authorities continue to ban inactive sites such as the political forum UAE Hewar and the blogs Secret Dubai Diary50 and UAE Torture.51 The latter had posted a torture video taken in 2004 in which a member of the ruling family was shown to have tortured an Afghan man. The suspect was acquitted in 2010 in a case that was widely believed to be a show trial.52 A request to unblock UAE Hewar was rejected by the Federal Supreme Court in July 2012, 53 and its Facebook page is also blocked due to its criticism of the regime and state corruption.54

As part of a verdict in which five users were sentenced to 7 to 15 years on charges of violating the constitution and cooperating with foreign political organizations (see “Prosecutions and Detentions”), a court also ordered the blocking of five websites that were already inaccessible in the country. These included the Emirates Media and Studies Center (EMASC); the Seven Emirates, which focuses on the seven activists who had their citizenship revoked for their political activities; the Watan news website; the Islah political group website; and the Yanabeea.net educational network.55

Over the past five years, political content has been the focus of state censorship. Examples include the secular pan-Arab online forum “Modern Discussion,”56 and the California-based Arabic online newspaper Watan, all blocked in September 2012.57 A website disseminating news of the trial of 94 Emirati political detainees was also blocked in 2013.58 The anonymous website UAE University Watch59 and UAE Prison, which exposes violations against jailed expatriates, have both been

44 “'Tinder-like': two expats launch new app for meeting people in the UAE.”
48 “Help us document blocket Internet Sites in UAE,” http://bit.ly/1e00dxW.
50 Secret Dubai diary (blog), http://secretdubai.blogspot.com/.
59 UAE University Watch, http://www.uaeuiversitywatch.net/.
United Arab Emirates

blocked. Emaraty Bedoon, the blog of the stateless individual Ahmed Abdulkhaleq who was deported to Thailand in July 2012 for his political activism, is also blocked.

Pages of political significance, such as the Arab-American news website Arab Times, the blog of an atheist Emirati man Ben Kerishan, and the anonymous Secret Dubai blog, continue to be blocked. In January 2014 alone, Twitter users have reported the blocking of ProxTube which unblocks censored YouTube content, the chatting website Omelga, and the image-based social network We Heart It.

The availability of Voice-over-Internet-Protocol (VoIP) services in the UAE is shrouded in doubt and complicated by disputes between the country’s two telecommunications companies, Etisalat and du, and the TRA. In the past, many aspects of VoIP applications were blocked by both providers, and Skype was classified by the TRA as an “unlicensed VoIP” When users landed on the Skype website, a notice appeared stating, “Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE’s Internet Access Management Policy.” In March 2015, providers blocked the Whatsapp voice calls feature a few hours after it was introduced. Two months later, Facebook’s video-calling feature was blocked as well. In April 2014, Etisalat’s Twitter account stated that Skype can only be used over Wi-Fi.

Similar products such as Viber or Apple’s Facetime have been banned since 2013; in fact, Apple agreed to sell its iPhone4 products to UAE mobile phone companies without the Facetime application preinstalled. Users in the UAE reported that Viber only works over Wi-Fi and Apple’s Facetime video-calling feature can only be used if the iPhone was purchased outside the country. However, on numerous occasions the TRA has emphasized that it is up to the mobile phone providers to license these products. In September 2014, the TRA clarified that the use of Viber and Skype in the country is still not permitted.

Etisalat and du currently offer their own prepaid VoIP cards, although their prices are higher than those listed by Skype. In January 2014, the VoIP service “Vippie by Voipswitch” tweeted that they were blocked in the Emirates. Despite these limitations, circumvention software and proxies are commonly used by Emiratis to access blocked content and VoIP services. However, the Dubai Po-
United Arab Emirates

lice declared the use of Virtual Private Networks (VPN) “illegal and punishable under the UAE law” in March 2015.75

BlackBerry services have been restricted since 2010, when the government introduced a regulation allowing only companies with more than 20 BlackBerry accounts to access the encrypted BlackBerry Messenger service.76 Two weeks after launching Blackberry’s BBM channels social media service in November 2013, the country’s two companies stopped the service in response to guidelines from the Telecommunications Regulatory Authority.77

According to a report from Citizen Lab in January 2013, ISPs in the UAE have used tools such as SmartFilter and NetSweeper to censor content. Citizen Lab also found five installations of Blue Coat ProxySG in the country’s network linked to Etisalat.78 Another report from CitizenLab in November 2013 listed websites that are blocked in the UAE because both SmartFilter (used by Etisalat) and NetSweeper (used by du) have miscategorized them as nudity or pornographic content.79 Although YouTube, Facebook, Twitter, and international blog-hosting services are freely available, controversial terms are often filtered from search results within these sites.

Content Removal

The removal of online content often lacks procedural transparency or judicial oversight. Under the 2012 cybercrime law, website owners and employees “may be held liable” for any violations occurring on their sites, including defamation charges.80

According to the Google Transparency Report for January to June 2014, the UAE authorities made two requests to remove Google+ posts that violated the 2012 cybercrime law. The posts were removed locally because they “contained obscene language and political satire against members of the ruling family of the UAE.”81 The report indicated that Google removed 85 percent of the 13 requests that were received in June 2014. Only two of those requests were court orders, according to the breakdown of data provided by Google.82

The Twitter Transparency Report indicated that no removal requests were made during the 2015 reporting period. However, one removal request was made during the January to June 2014 period specifying the removal of 13 accounts without a court order.83 In May 2012, Dubai police succeeded in shutting down 15 accounts on Facebook and Twitter for “defamation and abuse” by sending letters to both companies outlining the offenses committed under the UAE law.84

United Arab Emirates

Media, Diversity, and Content Manipulation

Local news websites, many of which are owned by the state, employ a large degree of self-censorship in accordance with government regulations and unofficial “red lines.” Gulf News, The National, and Emirates 24/7 are among the different online media outlets facing restrictions. The overall press freedom environment in traditional media is dire, with foreign journalists and academics often denied entry or deported for expressing their views on political topics.\(^{85}\)

Nonetheless, since the regional uprisings of 2011, Emiratis have begun to tackle sensitive issues more boldly over the internet, particularly on social media. Users express their opinions, share information on arrests and trials, and even attempt to organize protests. However, most users remain anonymous when criticizing state officials or religion out of fear of legal action or harassment. While there is no available evidence to prove the government’s involvement in hiring public relations firms or bloggers to spread propaganda, a large number of anonymous Twitter users appear dedicated to harassing and intimidating political dissidents and their families online.

In addition to the threat of harassment and prosecution, Emirati authorities also use financial means to limit the ability of antigovernment websites to produce content online. For example, the government reportedly pressured Dubai-based advertising agency Echo to end its advertising contract with the U.S.-based news outlet Watan. A complaint was also allegedly submitted to the FBI against the website, claiming it calls for the assassination of UAE rulers.\(^{86}\) Nonetheless, users have access to a variety of local and international news outlets, even if there are disparate reports of the blocking of specific UAE-related articles from these sites.\(^{87}\)

Digital Activism

Some Emiratis have continued to push back against government repression and intimidation by channeling their strong digital literacy into online activism, writing blogs, and calling for political reform on social networks. In the face of prosecution, activists still use online tools to highlight human rights violations and pass on messages from relatives in prison. Families of political prisoners still rely on Twitter to speak on behalf of detainees, explaining their cases, spreading information about violations of their rights, and calling for their release. There are several examples of relatives who are active online, including Mariam al-Mansouri,\(^{88}\) the wife of detained blogger Rashid al-Shamsi, and Aysha al-Thufiri, the daughter of detainee Salih al-Thufiri.\(^{89}\) Nonetheless, the online environment in the UAE is not free, and users face many challenges to freedom of expression online. For instance, three sisters were secretly detained for three months for tweets calling for the release of their detained brother Issa al-Suwaidi.\(^{90}\)

---


\(^{88}\) Mariam Mansori, Twitter Account, [https://twitter.com/MariamMansori](https://twitter.com/MariamMansori).

\(^{89}\) Aysha_75, Twitter Account, [https://twitter.com/Aysha_75](https://twitter.com/Aysha_75).

United Arab Emirates

Violations of User Rights

The rights of online users in the UAE are not protected by law, nor are they respected in practice. Several laws, including the penal code, the publishing law, and the cybercrime law, are commonly exploited to deter free expression and violate the rights of users. There is a general feeling among those who reside in the UAE that online tools are monitored and that surveillance is widely practiced with little judicial oversight. Several prominent online activists and ordinary citizens were detained in late 2012 and early 2013 as part of the UAE 94 trials. In addition, 2014 and 2015 saw a number of cases of arrest, torture, and long prison sentences.

Legal Environment

Article 30 of the UAE constitution states that “Freedom of opinion and expressing it verbally, in writing or by other means of expression shall be guaranteed within the limits of law.” However, the judicial system in the Emirates lacks independence, and prosecutions are often pursued for political reasons. Since the 2011 Arab Arising, the Gulf region made a collective effort to pass legislation that criminalizes criticism. As a result of this, the internet is heavily regulated in an attempt to quell legitimate free expression.

In August 2014, President Sheikh Khalifa bin Zayed al-Nahayan approved tougher antiterrorism measures. The passage of Terrorism Law No. 7 allows for severe punishments such as life imprisonment, death, and fines up to AED 100 million (US$27 million) if convicted as a terrorist. Under the law, citizens may be charged with such broad crimes as undermining national unity, possessing materials counter to the state’s notion of Islam, and “publicly declaring one’s animosity or lack of allegiance to the state or the regime.” The law had a chilling effect on free speech and paves the way for nonviolent opposition activists to be targeted for their views.

In a new decision by the country’s Federal Supreme Court issued in June 2015, insulting others via WhatsApp messages will be punished with an AED 250,000 (US$68,000) fine and jail time, with deportation for foreign violators.

The cybercrime law issued in November 2012 continues to be used to prosecute online users that are critical of the government. While the introduction of the law was fundamental in providing a sounder legal basis to combat online fraud, money laundering, hacking, and other serious cybercrimes, the law also criminalizes a wide range of online activity commonly accepted within international norms. For example, hefty fines and jail sentences await users who engage in online gambling, disseminate pornographic material, or violate another person’s privacy through posting their photograph or making statements about them online, regardless of the accuracy of the accusations. Intermediaries, such as domain hosts or administrators, are also liable if their websites are used to “prompt riot, hatred, racism, sectarianism, or damage the national unity or social peace or prejudice

the public order and public morals.” The cybercrime law also contains punishments for offending the state, its rulers, and its symbols, or for insulting Islam and other religions. Calls to change the ruling system are punishable by life imprisonment. Authorities have repeatedly warned foreign nationals that they must also follow the country’s restrictive laws.99

Articles 8 and 176 of the penal code are used to punish public “insults” of the country’s top officials, although these articles are also widely used to prosecute any users that express a desire for political reform.100 Articles 70 and 71 of the 1980 publishing law prohibit criticism of the head of the state and of Islam or any other religion.101 Defamation laws have been criticized by lawyers as “all-encompassing” and clouded with many grey areas. The burden of proof is also upon the defendant. Penalties can be as high as two years imprisonment or a fine of AED 20,000 (US$5,444).102

Prosecutions and Detentions for Online Activities

Since the sentencing of the 69 political dissents in 2013, the UAE continues to arbitrarily detain bloggers, netizens, and internet users. Human rights groups have continuously criticized the UAE for violating the human rights of political detainees and failing to provide them with fair and transparent trials. Instead, many are denied access to a lawyer, held without cause for extended periods of time, or tortured.103

Numerous Emirati users continue to serve long prison sentences for their online activities, mainly related to the UAE94 trials directed mainly against alleged members of the banned opposition movement al-Islah.104 Blogger Khalifa Al-Nuaimi105 and Twitter users Rashid al-Shamsi106 and Musabeh al-Rumaithy107 were arrested for their online activities and sentenced to 10 years imprisonment in July 2013. Blogger Abdullah al-Hajri108 and Twitter user Omran al-Radhwan109 are serving seven-year sentences.110

Several Emiratis were sentenced to prison for criticizing state institutions, particularly over their criticisms of the UAE94 trials.

- In November 2014, online activist Osama Al-Najjar was sentenced to three years in prison

105 Al-Nuaimi had previously written about “the UAE 5” and had been consistently threatened prior to his arrest: "( درغملا لبق ميظنتلا نع فشكي .. ) حبصموب !! Kalnuaimi (blog), July 15, 2012, http://bit.ly/1jqEuCW.
106 al-Shamsi had tweeted news of arrests and written blog posts related to politics and free speech See Rashed Al Shamsi (blog), http://bit.ly/1hG88O.
107 al-Rumaithy was arrested for his online writings in which he expressed support for the Islamist Islah party. He had been handed a travel ban one month before his arrest. See GC4HR, “UAE- Travel bans imposed against human rights activists as restriction on freedom of movement increases,” July 1, 2012, http://www.gc4hr.org/news/view/187.
108 Al-Hajri was arrested over the contents of his blog, http://allhajria.wordpress.com_in which he called for more government action to combat public immorality.
109 Al-Radhwan had tweeted about “the UAE 5” detainees and wrote several posts on his website, http://omran83.tumblr.com_promoting Islah and criticizing state violations of Shariah law.
and fined US$136,000 for tweets alleging that his father, who was imprisoned as part of the UAE94 trials, was tortured by security forces. 111 Osama Al-Najjar had been arrested in March 2014 and was detained without trial until September 2014, after the passage of the new antiterrorism law. He was found guilty of belonging to banned political group al-Islah, spreading lies, and instigating hatred against the state through Twitter.112

- Similarly, in June 2015, Nasser al-Faresi was sentenced to three years in jail for a tweet insulting the Federal Supreme Court and the ruler of Abu Dhabi. The court charged him with “spreading rumors and information that harmed the country.”113

This continues a trend from last year:

- Mohammed Salem al-Zumer is currently serving a three-year sentence since December 2013 for his posts on Twitter and YouTube regarding the UAE94 trials.114

- Abdulrahman Bajubair was sentenced to five years in jail for running a blog and Twitter accounts reporting on the mistreatment of political detainees in December 2013.115

- In March 2014, Khalifa Rabeiah and Othman al-Shehhi were fined and are currently serving a five-year sentence for tweets critical of the judiciary system.116

Several noncitizens were arrested for social media posts under the country’s harsh cybercrime laws:

- In April 2014, authorities arrested and deported Palestinian refugee and human rights advocate Iyad el-Baghdadi to Malaysia because of his Twitter activism.117 Details of el-Baghdadi’s ordeal only surfaced in October 2014, when he was finally able to leave Malaysia for Norway to attend an event and apply for political asylum.118

- In February 2015, Ryan Pate, an American contractor in the UAE was arrested upon arrival for a Facebook post insulting the country and his employers.119

- In July 2015, Jodi Magi, an Australian national was deported from the UAE after posting a picture to Facebook showing a vehicle blocking disabled car spaces.120 Magi was arrested in March 2015 and released on bail before being convicted under the cybercrime law.121

Other cases from the coverage period include:

119 Stephanie Gallman, “Florida man arrested in UAE for Facebook post: I’m sorry,” CNN, March 5, 2015, http://cnn.it/1w85KuT.
United Arab Emirates

- In March 2015, an Emirati man and woman were arrested after a pornographic video of them circulated online. Dubai court sentenced them both to one year in jail, while a third defendant was charged with an unspecified sentence for circulating the material.\footnote{Salam Al Amir. “Pair sentenced in Dubai after their sex video circulates on the internet,” The National, March 5, 2015, http://bit.ly/1OF73ns.}

- In October 2014, a man was fined AED 10,000 (US$2,700) by Sharjah court for insulting a woman on a news website. The court’s decision concludes that because the internet is available throughout the country, an online offense can be tried in any of the Emirates even though the website’s company is based in Dubai.\footnote{Haneen Dajani. “Online verbal insults are punishable in any emirate, UAE Supreme Court rules,” The National, October 27, 2014, http://bit.ly/1PjepZP.}

- In June 2015, the Federal Supreme Court used the 2012 cybercrime law to order the retrial of a man convicted of insulting his colleague via WhatsApp. The defendant might face a US$68,000 fine as authorities warned of imprisonment and deportation if similar cases happen in future.\footnote{“UAE man faces $68,000 fine for swearing on WhatsApp,” BBC, June 16, 2015, http://bbc.in/1d0syDV.}

According to Dubai Police, in 2014, 212 cases of extortion and blackmail via social media had been reported compared to 80 in 2013.\footnote{“UAE in crackdown on social media abuse,” Arabian Business, March 10, 2015, http://bit.ly/1FKCuW.}

Surveillance, Privacy, and Anonymity

The high amount of prosecutions and physical harassment of users in the UAE is, in part, due to the obstacles they face in using ICT tools anonymously. Mobile phone users re-registered their information as part of a 2012 TRA campaign “My Number, My Identity.”\footnote{The TRA’s statement reads: “Your mobile phone number is an extension of your identity. Sharing or giving away your SIM-Card to others can cause unwanted consequences, including being held accountable for any improper conduct or misuse associated with the mobile phone subscription by the authorities as well as being liable for all charges by the licensees: Telecommunications Regulatory Authority,” My Number My Identity,” accessed April 28, 2013, http://bit.ly/1LPbs66; and Nadeem Hanif, “Every mobile phone user in the UAE must re-register SIM card,” The National, June 28, 2012, http://bit.ly/1k7EfoY.}

In January 2013, the country’s two mobile phone providers issued a final warning to their users to register their SIM cards or have their lines cut for failing to comply.\footnote{Nadeem Hanif, “Du and Etisalat brace for UAE users last chance to re-register Sim card,” The National, January 16, 2013, http://bit.ly/1GeZoq.}

Cybercafe customers are also required to provide their ID and personal information in order to surf the net.\footnote{Morgan Marquis-Boire, et. al., Planet Blue Coat: Mapping Global Censorship and Surveillance Tools, Citizen Lab, January 15, 2013, http://bit.ly/1d08WPY.}

In April 2014, the Ministry of Interior announced plans to link ID cards with internet services and cellphones “to crackdown on child abusers.” An official stated “by linking ID cards with internet service providers, people’s identities will be linked to the websites they visit.”\footnote{Caline Malek, “UAE ministry to link ID cards with the internet to crack down on child abusers,” The National, April 5, 2014, http://bit.ly/1LPc4J0.}

In March 2015, the TRA announced its establishment of an alert system that detects certain keywords relating to “nudity, sexual cyber-extortion and insulting members of the ruling families.” Ghaith Al Mazaina, acting manager at the security quality service at the TRA, stated: “We have started monitoring all the social media channels – all websites and profiles are monitored.” Another TRA official added: “We try
United Arab Emirates

to get the page or profile down or remove the violation as soon as possible and report the case to police if it is a criminal case.130

Internet and mobile providers are not transparent in discussing the procedures taken by authorities to access their data and users' information. Incidents of providers demanding warrants or legal permissions for security bodies to gain access to user data are not known. Warnings from both the Abu Dhabi and Dubai police against spreading rumors through mobile messages may indicate the government's overall surveillance on users.131

Twitter users have been arrested for exchanging private messages with controversial accounts.132 For example, Saeed al-Shamsi was detained on December 14, 2012 over suspicions that he ran the anonymous Twitter account called “Sout al-Haq” (@weldbudhabi). The account was targeted over allegations that it received leaked documents from the Interior Ministry, although the documents were never published. After al-Shamsi's arrest, the Sout al-Haq account sent a tweet in which he claimed the authorities had arrested the wrong person. Al-Shamsi’s lawyer said that his defendant appeared distressed and disoriented in court with signs of intimidation and torture.133 He was reportedly released in March 2013. Two other users were also arrested for having messaged Sout al-Haq after authorities reportedly hacked into the account. Only days after, five more Twitter users were arrested for expressing political criticism and support for detainees.134

Intimidation and Violence

Online activists in the UAE face arbitrary detention, travel restrictions, and potentially torture. In February 2015, Emirati authorities arrested Omani blogger Muawiyah Alrawahi as he was crossing into the country by car. The blogger has been critical of both Omani and UAE authorities online and remains in arbitrary detention as of July 2015.135 Human rights defender Ahmed Mansoor has faced continual harassment by the authorities, and is subject to a travel ban.136 Similarly, three sisters disappeared in February 2015 shortly after being questioned for posting tweets on behalf of their brother, Dr. Issa al-Suwaidi (part of the UAE 94), who is currently a prisoner of conscience.137 Asma Khalifa al-Suwaidi, Mariam Khalifa al-Suwaidi, and Dr. Alyaziya Khalifa al-Suwaidi were released three months later in May.138

Technical Attacks

Emirati activists have reported spyware and malware attacks against their computers. In October

133 Donaghy, “Torture in the United Arab Emirates.”
134 Law, “Eight online activists ‘arrested in UAE’.”
136 GC4HR, Hear their Voices: Alarming Times for Human Rights Defenders in the Gulf Region & Neighboring Countries.
2014, the Twitter account of human rights defender Ahmed Mansoor was hacked, with some blaming state security. In one case from January 2013, a user received an e-mail purportedly containing a link to a video of the Dubai police chief. Instead, the link contained spyware that could monitor the victim’s screen, enable the computer’s webcam, steal passwords, and conduct keylogging. It was believed the Emirati government was behind the attack.

The UAE remains one of the top countries facing hacking attempts worldwide. According to a study by Kaspersky Lab, the UAE is the second most attacked country online in the Middle East and the 15th most attacked worldwide. The country’s spam rate was recorded at 73 percent, and 46 percent of the country’s social networking users fell victim to cybercrimes, compared to the global average of 39 percent. Kaspersky Lab has also reported that 51 per cent of users in the UAE faced financial cyber-attacks during 2014, with 10 per cent of respondents reportedly losing money as a result.

In August 2014, the Dubai Financial Services Authority said it has issued nine alerts warning firms about the scams, which use the internet to impersonate genuine investment companies and individuals, adding that such abuse is on the rise. In January 2015, Abu Dhabi Police warned against scam bank reports received by email, claiming suspicious money transfers to users’ bank accounts. In July 2015, the technology company Symantec was able to uncover a new corporate espionage group that has compromised a string of major corporations in recent years, including three organizations located or headquartered in the UAE.

---


United Kingdom

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population:</td>
<td>64.5 million</td>
<td></td>
</tr>
<tr>
<td>Internet Penetration 2014:</td>
<td>92 percent</td>
<td></td>
</tr>
<tr>
<td>Social Media/ICT Apps Blocked:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Political/Social Content Blocked:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Bloggers/ICT Users Arrested:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Press Freedom 2015 Status:</td>
<td>Free</td>
<td></td>
</tr>
</tbody>
</table>

| Obstacles to Access (0-25) | 2 | 2 |
| Limits on Content (0-35) | 6 | 6 |
| Violations of User Rights (0-40) | 16 | 16 |
| TOTAL* (0-100) | 24 | 24 |

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- In February 2015, English and Welsh law was amended to criminalize pornographic images distributed online without the subject’s permission and with the intent to harm the subject, so-called “revenge porn.” The law, which went into effect in April 2015, made the offense punishable by up to two years in prison, an increase from six months (see Legal Environment).

- In what seems to have been the first instance in the UK of a revenge porn prosecution, a 21-year-old was sentenced to 12 weeks in jail in November 2014 for threatening a woman and disseminating naked photographs of her without her permission via social media (see Prosecutions and Detentions for Online Activities).

- Alaa Esayed, an Iraqi national living in the UK, was charged with publishing and disseminating terrorist material via Twitter and Instagram in December 2014, resulting in a three-and-a-half-year prison sentence in June 2015. While she argued she was simply “cutting and pasting” other people’s messages, the court held that their dissemination encouraged young people to travel to foreign countries in order to commit terrorist acts (see Prosecutions and Detentions for Online Activities).

- In February 2015, the Investigatory Powers Tribunal ruled that the Government Communications Headquarters (GCHQ) had acted unlawfully in accessing information on millions of individuals collected by its U.S. partner, the National Security Agency (NSA), prior to December 2014 (see Surveillance, Privacy, and Anonymity). As a result, Privacy International set up an online tool through which users can ask the tribunal if the GCHQ has illegally monitored their activities (see Digital Activism).

- Shortly after the terrorist attacks in Paris in January 2015, Prime Minister David Cameron called for a ban on encryption in messaging apps. While the move was met with criticism from internet freedom and security activists who argued that it would be highly impractical, the government continued its plans and put forward a draft investigatory powers bill, dubbed the “snoopers’ charter” by activists (see Surveillance, Privacy, and Anonymity).
Introduction

Online harassment, extremist speech, and privacy were the three main issues seen in internet policy in the United Kingdom (UK) over the past year. The UK was an early adopter of new information and communication technologies (ICTs), and internet access in the country has become near universal with competitive prices and generally fast speeds. Internet access through mobile phones is also becoming more prevalent as a result of the growing popularity of smartphones and the increasing availability of superfast networks. But the growth in technological capacities has simultaneously allowed expanded surveillance, leading to mounting fears of abuse by police and intelligence agents.

In February 2015, the Investigatory Powers Tribunal ruled that the Government Communications Headquarters (GCHQ) had acted unlawfully in accessing information collected by its U.S. partner, the National Security Agency (NSA), prior to December 2014—before the GCHQ practices were made public. The decision marked the first time the tribunal has ruled against any of Britain’s three intelligence agencies—GCHQ, MI5, and MI6—that it is entrusted to oversee.

In another positive development, a government-commissioned report released in June 2015 found that the existing legislative framework on surveillance was "undemocratic, unnecessary and—in the long run—intolerable." David Anderson QC, the author of the report, recommended halting any new legislative proposals on surveillance until they were assessed for "lawfulness, likely effectiveness, intrusiveness and cost." However, continued statements by Prime Minister David Cameron highlight the government’s worries over improved encryption standards. The new director of GCHQ referred to U.S. technology companies such as Twitter, Facebook, and WhatsApp as "command-and-control networks…for terrorists and criminals" and called for greater cooperation between companies and security agencies.1

Obstacles to Access

Access to the internet is considered to be a key element determining societal and democratic participation in the United Kingdom (UK).2 ICT infrastructure in the country is generally strong, allowing high levels of access: the overwhelming majority of UK citizens use the internet frequently on a widening variety of devices. In recent years there have been substantial investments in superfast broadband, led by the government’s Rural Broadband Programme,3 which has led to better levels of service for many citizens and businesses. For financial and literacy reasons, however, there is still a small segment of the population that does not have internet access, specifically those over 75 and people in the lowest socioeconomic groups.4 Policies and regulation in the country tend to favor access, although continuing revelations regarding extensive government surveillance practices may impact how citizens choose to access the internet.

---

4 Ofcom, Internet Citizens 2014, p.11
Availability and Ease of Access

Internet penetration has grown to 85 percent as of early 2015, with the share of homes with fixed and mobile broadband at 80 percent.\(^5\) Three in ten of all broadband connections are labeled as “superfast,” meaning they have an advertised speed of at least 30 Megabits per second (Mbps).\(^6\) Nearly 100 percent of all households are within range of ADSL connections. The government’s Rural Broadband Programme has now been incorporated within a larger Superfast Broadband Programme, and funding expanded to GBP 1.7 billion (US$ 2.62 billion) aimed at improving broadband speed and access.\(^7\) As of March 2015, an additional 2,411,395 premises had access to superfast broadband through the scheme, meaning a total of 80 percent of all UK premises had superfast broadband access availability, in line with a target of 95 percent by 2017.\(^8\) So, while broadband access is effectively ubiquitous, steady progress continues towards the aim of superfast broadband in all areas, which is a stated priority.\(^9\)

Mobile telephone penetration is extensive, with a reported penetration rate of 123.58 percent at the end of 2014.\(^10\) In 2014, 66 percent of all UK adults claimed to own a smartphone, reflecting a substantial growth of internet use on mobile phones.\(^11\) The fastest growth in mobile internet use was among people aged 55 to 64, which increased more than five-fold in four years. Fourth-generation (4G) mobile communication technology is now available from all four national mobile network operators, with more than 23 million subscriptions and over 89 percent of UK premises being able to access outdoor 4G coverage from at least one network.\(^12\) Second-generation (2G) and third-generation (3G) networks are available in over 99 percent of all households. At 33 percent, smartphones were the most important device for internet access as of mid-2015, surpassing laptops (30 percent) and tablets (19 percent).\(^13\)

Even where access is available, use and participation does not necessarily follow. Citizens with internet access may choose not to participate if they lack technical understanding or adequate equipment, if they are concerned about privacy online, or if they have no interest in being online. People in the lowest income groups are significantly less likely to have home internet subscriptions, with the gap between socioeconomic groups remaining the same for the past few years. People aged 75 and above are also less likely to use the internet, although internet use by this group has increased since 2008.\(^14\) Of the UK households that do not have access to the internet, the majority have no intention to get connected.\(^15\) There is a no gender gap in internet use.

---


\(^6\) Ofcom, *The Communications Market Report*, August 6, 2015, p.3

\(^7\) DCMS, *2010 to 2015 government policy: broadband investment*, Appendix 2


\(^9\) For local area progress in broadband provision, see DCMS, *Table of local broadband projects*, October 2014, [https://docs.google.com/spreadsheet/ccc?key=0Ah3sVRlTB2kD9m6hXOUJd3lWWhNbj8nNGvxeHqMHc#gid=0](https://docs.google.com/spreadsheet/ccc?key=0Ah3sVRlTB2kD9m6hXOUJd3lWWhNbj8nNGvxeHqMHc#gid=0)


\(^12\) Ofcom, *The Communications Market Report*, August 6, 2015, p.1


United Kingdom

The average broadband speed in November 2014 was 22.8 Mbps, continuing a trend of rising speeds and growing satisfaction among consumers served by faster fiber-optic based services. The introduction of 4G services for mobile in 2012 has allowed faster data downloads and uploads, streaming of video, and access to other data services. A total of 61 percent of adults said they used data services on their mobile phones, a four percent increase from 2014. The 7.1 million fixed broadband lines providing speeds of 30 Mbps or higher in the UK today account for 30 percent of all fixed broadband lines, compared to 0.2 percent in 2009. Superfast connections are increasingly deployed beyond the major urban centers, and the price of such connections is decreasing.

The UK provides a competitive market for internet access, and prices for communications services compare favorably with those in other countries. Average fixed internet spending has continued to increase as a result of a growth in broadband uptake and the rise of superfast services. While 4G services were initially more expensive than non-4G services, the difference is shrinking, and in some cases disappearing. The price basket of mobile services continues to fall in real terms, specifically by 0.4 percent in 2014, and is around GBP 14.30 (US$ 21.90). The difference between superfast and standard services in 2014 was between GBP 5 (US$7.66) and GBP 10 (US$15.31) per month.

Economic constraints do appear to negatively impact older and poorer users’ ability to participate online. While 85 percent of the UK population has access to internet in their homes, as of 2014 only 63 percent of individuals over the age of 65 use the internet, and among those in the lowest socio-economic group, including the unskilled manual labourers and long-term state dependents, only 64 percent self-describe as internet users.

Restrictions on Connectivity

The government does not place limits on the amount of bandwidth ISPs can supply, and the use of internet infrastructure is not subject to direct government control. ISPs regularly engage in traffic shaping or slowdowns of certain services (such as peer-to-peer file sharing and television streaming), and can also be made to block-access to specific sites via court orders. Mobile providers have cut back on previously unlimited access packages for smartphones, reportedly because of concerns about network congestion.

ICT Market

The five major internet service providers (ISPs) are British Telecom (BT) with a 32 percent market share, Sky (22 percent), Virgin Media (20 percent), TalkTalk (14 percent), and EE (4 percent). Through local loop unbundling—where communications providers offer services to households using infrastructure provided mainly by BT and Virgin—a large number of companies provide internet

---

16 Ofcom, The Communications Market Report, August 6, 2015, p.15
17 Ofcom, The Communications Market Report, August 6, 2015, p.340
18 Ofcom, The Communications Market Report, August 6, 2015, p.15
21 Ofcom, The Communications Market Report, August 6, 2015, p.317
24 Ofcom, The Communications Market Report, August 6, 2015, p.292
access. By 2013, unbundled telephone lines reached 9 million homes. Virgin has the highest share of superfast broadband subscribers at 56 percent as of 2014; BT has a 35 percent share, but is dominant in the provision of wholesale access. ISPs are not subject to licensing but must comply with general conditions set by the communications regulator, Ofcom, such as having a recognized code of practice and being a member of a recognized alternative dispute-resolution scheme.

The telecommunications provider O2 leads the mobile operator market, with some 22 percent of market, followed by Vodafone (19 percent), Orange (11 percent), and Three (3) (10 percent) according to information from Statista as of 2014.

Regulatory Bodies

Ofcom is the primary regulator, by virtue of the broad definitions of responsibility for “citizens,” “consumers,” and “communications matters” granted to it under the Communications Act 2003.

In July 2012, major ISPs published a “Voluntary Code of Practice in Support of the Open Internet.” The code commits ISPs to transparency and confirms that traffic management practices will not be used to target and degrade the services of a competitor. The code was amended in May 2013 to clarify that signatories could deploy content filtering or provide such tools where appropriate for public Wi-Fi access.

In September 2013, the domain registrar Nominet launched a review of the “.uk” domain registration policy to focus on the extent to which it should restrict offensive or otherwise inappropriate words or expressions in domain name registrations. The Nominet Board agreed to all the recommended changes, which included a post-registration domain name screening to suspend or remove domain names that encourage serious sexual offenses.

In addition, the Internet Watch Foundation (IWF), an independent self-regulatory body funded by the EU and the online industry, provides a UK internet hotline for the public and IT professionals to report criminal online content in a secure and confidential way. A range of other self-regulatory bodies—for example, the Video On Demand Association, a private self-regulatory body with responsibility for regulating video content in keeping with the EU AudioVisual Media Services Directive, the
United Kingdom

Advertising Standards Authority, and IPSO, which regulates newspaper websites—apply a combination of voluntary ethical codes and co-regulatory rules to internet content. With the exception of the filtering and blocking blacklists dealing with child abuse content (which are agreed upon by the IWF) these bodies eschew pre-publication censorship and operate post publication notice and takedown procedures within the E-Commerce Directive liability framework.

Limits on Content

The United Kingdom has no blanket laws covering internet blocking but various categories of criminal content such as depictions of child sexual abuse, promotion of extremism and terrorism, and copyright infringing materials are blocked by ISPs using filtering tools. Meanwhile parental controls over adult-oriented sites have become the default, requiring adults to opt-out of the filtering technology to access adult material. These measures have been considered controversial as they often result in over-blocking, and a lack of transparency persists regarding the sites blocked.

Blocking and Filtering

The government has thus far taken a proactive approach to restricting sites that have been found in violation of copyright protections, indicating possible further action to curb infringement. The UK High Court blocks sites based on copyright violations, but it recently held that publishing a link to copyright infringing material, rather than actually hosting it, does not amount to an infringement. This approach was confirmed by the Court of Justice of the European Union. There have been a number of cases in which courts have ordered sites, such as Newzbin and The Pirate Bay, to be blocked for infringing copyright, and to have their domain names seized based on legislation like the Copyright, Designs, and Patents Act.

The CleanFeed system has also been expanded so the blocks can be enforced by ISPs. The list of violating websites has been growing continually. The Digital Economy Act (DEA) of 2010 states that a court order can block sites containing “substantial” violations of copyright. However, as a response to an Ofcom review, which determined that such copyright-related blocking provisions, stipulated in Sections 17 and 18 of the DEA, are unlikely to be effective alone and should rather be used in conjunction with other measures, representatives from the UK’s creative industries and major Internet Service Providers (ISPs) have come together with the support of government to launch Creative Content UK.

Creative Content UK was launched in Spring 2015, and comprises a major multi-media education awareness campaign, that aims to create wider appreciation of the value and benefits of entertainment content and copyright. The second component is a subscriber alerts program that will be co-managed and co-funded by ISPs and content creators and is due to begin at a later date. The UK’s Department for Culture, Media and Sport (DCMS) has indicated that the program will replace the unfavorable anti-piracy regime rushed through under the DEA where the Secretary of State for

---

36 Sajid Javid’s speech at British Phonographic Industry AGM, Department for Culture, Media and Sport, 1 September 2014, http://bit.ly/1atulAP
United Kingdom

Culture, Media and Sport is able to facilitate “blocking injunctions” by the courts in order to force ISPs to block access to pirated copyright content. Nonprofit groups like Open Rights Group (ORG) had criticized regulatory reliance on the DEA approach, as obtaining copies of the copyright injunctions has proved challenging. Consequently, ORG has called for more transparency about what sites are blocked by court injunctions.

UK blocking policy is instituted in accordance with a voluntary code of practice set forth by the Internet Services Providers’ Association. British ISPs are not required by law to implement the IWF blocking list, however since 2010, the Home Office has instituted rules prohibiting government bodies from working with ISPs that fail to use the list. Consumer awareness of CleanFeed remains low, with the list of blocked sites kept from the public in an effort to deter access to unlawful materials. In January 2014, a human rights audit of the IWF recommended that an independent judicial review of IWF’s operations be conducted.

In November 2013, Google and Microsoft introduced new algorithmic filters that prevent searches for child abuse imagery. Around 100,000 terms for illegal material are programmed to yield no search results. At the same time, laws like the Protection of Children Act are used to prosecute individuals suspected of accessing or distributing content containing sexual abuse of children. According to reports by civil society groups, the filters raise transparency concerns and evade reporting requirements under the Freedom of Information Act, particularly regarding how these filters work and why certain sites may be blocked without court orders.

In the face of rapidly increasing mobile uptake in the UK, mobile filtering has also become increasingly prevalent. Concerns have also grown over the unsupervised use of data-enabled mobile phones by children under the age of 18, which has led to mobile internet subscriptions being sold to customers with child filters enabled by default, and access to adult content requiring users to verify their age to ‘opt-in’. The May 2015 elections featured commitments made by the Conservative Party, which won a parliamentary majority, to strengthen internet porn filters. Blocked content categories, which include pornography, hate sites, and in some cases, web forums that could potentially allow minors to interact with older users, are set out in the 2004 code of conduct established by the Mobile Broadband Group (MBG), consisting of the providers Vodafone, Three, EE, and O2. The code of conduct, last updated in July 2013, covers commercial and internet content, illegal content, malicious communications, and customer education. In September 2013 the British Board of Film Classification (BBFC) replaced the Independent Mobile Classification Body (IMCB) in categorizing content and calibrating internet filters. However, the process continues to be criticized for being too subjective and lacking transparency.

In November 2013, Sky, TalkTalk, BT, and Virgin led a joint awareness campaign around child safety, launching the InternetMatters.org portal in May of 2014 with the aim to provide parents with advice regarding children’s online safety. The efficacy of these child-protection measures for filtering content on both mobiles and household access has been questioned. They can not only be easily circumvented with minimal effort, but have been known to lead to the over-blocking of legitimate content. For example, due to technical glitches at the ISP level, users were barred from accessing popular sites such as Wikipedia. In response, ORG created the site “Blocked.org.uk” to allow users to report over-blocking of content that poses little or no threat to child welfare, including sites on

39 ‘ISPs collaborate with music and film industries on voluntary scheme to combat online piracy,’ SnlPPts, 13 May 2014 http://bit.ly/1KmteC
sexual education, homosexuality and drug awareness, and pages run by civil society and political parties. The website of the British National Party, an extreme right-wing political organization, was temporarily blocked for being classified by O2’s filter system as a “hate site.” As O2 is the only large ISP that operates an “URL checker” page that allows users to ascertain how a particular site has been classified, genuine concerns arise around owners and operators of sites not being notified that their sites have been blocked. ORG reports that some cases of sites blocked on mobile networks have taken a month to be resolved, and that site operators often do not know where to report a wrongfully blocked site.

Content Removal

The government has stepped up efforts to curb radicalization on the internet. The Terrorism Act calls for the removal of material hosted online in the UK if it “glorifies or praises” terrorism, could be useful to conducting terrorism, or incites people to carry out or support terrorism. A Counter Terrorism Internet Referral Unit (CTIRU) was set up in 2010 to investigate internet materials and take down instances of “jihadist propaganda.” The government updated its “Prevent Anti-Terrorism Strategy” in 2015, which calls for limiting access to “extremist” materials online through school and public library networks and increasing efforts to remove “harmful content” from the internet. The strategy involves “sharing unlawful sites for inclusion in commercial filtering products,” through the compiling of a list of extremist URLs by the CTIRU that are then blocked by ISPs.41 (see also, “Blocking and Filtering” above.)

The Internet Watch Foundation (IWF) compiles a blacklist of URLs with visual depictions of child sexual abuse to prevent access to such illegal content. A citizen’s hotline combined with investigations by IWF analysts in accordance with the Sexual Offences Definitive Guideline published by the Sentencing Council under the Ministry of Justice is used to discover and evaluate illegal sites. When the content in question is hosted by UK servers, where this constitutes a criminal offense, the IWF coordinates with the police and local hosting companies to remove it. A similar system exists for websites containing child sexual abuse through non-photographic means, such as computer-generated images, as well as for websites with criminally obscene adult content.

For content that is hosted by overseas servers, the IWF coordinates with international hotlines and police authorities to get the offending content taken down in the host country. In the meantime, British users are prevented from accessing content deemed illegal by British ISPs using the CleanFeed filtering system, which was developed by the IWF and BT. Similar processes are in place for the investigation of online materials inciting hatred under the oversight of TrueVision, a site that is managed by the police.

According to the EU 2002 E-Commerce Directive, knowledge of illicit material, including libelous content, on a host website in conjunction with a failure to remove it is prosecutable. This has resulted in hasty takedowns by hosting companies, with little inquiry as to the legitimacy of the takedown notice. In April 2013, the government updated the Defamation Act. The updates came into effect on January 1, 2014, and provide greater protections for ISPs by limiting their liability for user-generated content.

United Kingdom

Although EU rather than UK-specific, the so-called “right to be forgotten” ruling from the European Court of Justice in May 2014, which gave search engines the task of removing links from their search results on the requests of individuals if the stories in question were deemed to be inadequate or irrelevant, has had an impact on the way content is handled in the country. According to Google’s Transparency Report on European privacy removal requests, Google had received 35,140 requests by July 2015, requesting the removal or 137,955 URLs from its search results. The rate of compliance was 37.5 percent. News publishers including the BBC and the Telegraph have retaliated by publishing lists of the stories which had been delisted by search engines. In May 2015, it was reported that the Information Commissioner’s Office was in talks with Google over cases that it believed the search engine had not resolved effectively.

Media, Diversity, and Content Manipulation

Self-censorship is difficult to measure in the United Kingdom, but not a grave concern. After the January 2015 attack on the French publication Charlie Hebdo some publications refrained from publishing the controversial cartoons of the prophet Muhammad, but these were not government influenced or mandated. Due to the UK’s extensive surveillance practices, it is possible that certain online groups feel as though they must self-censor to avoid potential government interference.

In June 2015 the UK’s Investigatory Powers Tribunal confirmed that GCHQ had been unlawfully surveilling NGOs, including Amnesty International and Legal Resources Center in South Africa. The tribunal made “no determination” on the claims brought by other NGOs, including Liberty and Privacy International, which could mean either that GCHQ is not surveilling the two NGOs, or that the surveillance has been deemed lawful. Representatives from Amnesty International, Privacy International, and Liberty alluded to the possibility of self-censorship by stating that they could not appropriately do their job under such conditions of surveillance.

Other than surveillance, and the government’s role in encouraging the filtering activities described above, there is no explicit evidence relating to the government manipulation of online content. Online media outlets face economic constraints that negatively impact their ability to remain financially sustainable. Publications have struggled to find a profitable system for their online news platforms as ad revenue continues to fall.

The UK telecoms regulatory, Ofcom, adopted a voluntary code of practice on broadband speeds in 2008 and released a report in 2011 that called for a self-regulatory approach to network neutrality. It described the blocking of services and sites by ISPs as “highly undesirable” but said that market

---

43 Neil MacIntosh, List of BBC web pages which have been removed from Google’s search results, BBC Internet Blog, June 25 2015 http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02bf7fd379
48 http://rt.com/uk/271111-gchq-amnesty-international-spy/
United Kingdom

Forces will address potential problems. Developments at European Union (EU) level are likely in the future to have an impact on net neutrality provisions in the UK, after agreement has been reached to ban paid prioritization across the EU as part of the Digital Single Market policy package.

There are a wide variety of news platforms available online, with 60 percent of people reporting that they consume news online, and 44 percent reporting that they consume news through apps. Blogs and social media also act as available news sources, but have seen a readership decline by four points to 23 percent. Diverse views are present online, but may not be widely read, as 59 percent obtain their news from the BBC website or app, 18 percent obtain their news through Google, and 17 percent obtain their news through Facebook.

Digital Activism

Online political mobilization continues to grow both in terms of numbers of participants and numbers of campaigns, though the efficacy of online mobilization remains controversial and it is impossible to explain success with reference to online campaigns alone. Petition and advocacy platforms such as 38 Degrees and AVAAZ continued to grow, with AVAAZ claiming around 1.6 million “members” in 2015 in the UK. All civil society organizations, charities and political parties now view online as an indispensable part of a wider campaign strategy.

As a result of Privacy International’s case against the Investigatory Powers Tribunal (IPT), British citizens are now able to find out if they were illegally spied on by applying directly to the IPT, which is obligated to respond to any complaints and reveal if an individual was illegally monitored. If so, the individual can ask that the data be deleted. Privacy International has made this process even more accessible, by providing a form on its website for applicants, which it will submit on their behalf and fight in any resulting court battles. More than 6,000 people signed up in the first 24 hours after the form was launched, which topped 10,000 in the first two days.

Violations of User Rights

The government has placed significant emphasis on stopping the dissemination of terrorist and hate speech online and on protecting individuals from targeted harassment on social media. While, changes to civil liability laws implemented through the Defamation Act 2013 were meant to relieve content producers and website operators of the burden of ever-loomng threats of libel action, the benefits have so far seemed unrealized. Furthermore, users’ rights still seem caught in the shadow of extensive surveillance measures used by the government to monitor the flow of information for law enforcement and foreign intelligence purposes. There were several notable legal changes over the past year in these areas.

---

United Kingdom

Legal Environment

The UK currently has no constitution or bill of rights, relying instead on the provisions of the European Convention on Human Rights (ECHR), which have been adopted into law via the Human Rights Act 1998. However, in the fall of 2014, Conservative Party officials, including the prime minister, announced their intentions to repeal the Human Rights Act in favor of a UK Bill of Rights in order to give British courts more control over application of human rights principles. Furthermore, following the election of a Conservative government in May 2015, the prime minister reiterated his position that he remains open to withdrawing from the ECHR entirely should parliament not successfully secure the ability to veto decisions of the European Court of Human Rights.

In September 2015, with a new government in office after the general elections that year, the home secretary outlined a proposal for “extremism disruption orders.” The orders would allow judicial review of individuals and groups who “spread hate but do not break laws,” disallowing them from posting messages to social media without first gaining government approval. While much discussion has centered around combating terrorism, officials have noted that the orders could be used to limit speech of those groups found to disseminate hatred based on gender, sexual orientation, religion, and disabilities. That proposal, supported by the prime minister, also included plans to grant Ofcom, the broadcast and telecommunications regulatory authority, powers to prevent broadcast of “extremist messages,” requiring pre-transmission monitoring of content. However, this proposal has met vocal opposition even from within the Conservative Party, including at least four cabinet ministers in the newly elected government.

Beyond targeting extremist and hate speech, the UK has focused on online harassment as well. In February 2015, the Criminal Justice and Courts Act 2015 amended section 1 of the Malicious Communications Act 1988 to quadruple the possible time in prison to two years in the case of targeting individuals with abusive and offensive content online “with the purpose of causing distress or anxiety.” The new law, effective in England and Wales only, opened the crown court for more serious offenses, whereas previously only the magistrates’ courts may hear such cases. The changes also extended the time limit to bring charges for these offenses to three years from the date of the of-

Going further, though, in order to combat such trolling, revenge porn, and other such cyber-bullying, a House of Lords committee recommended in a July 2014 report that websites allowing individuals to post content should be required to establish the actual identity of such individuals beforehand before permitting them to post under a pseudonym or anonymously. Critics argue that such a measure would chill important speech by removing the protections of anonymity from those otherwise afraid to speak. While no specific action on this report’s recommendation has been taken, the Defamation Act 2013 offers protection to website operators from private libel suits based on third-party postings only if the alleged victim of defamation can find the user. While the act does not specify what sort of information the website operator must provide to plaintiffs, unauthenticated identity information may be falsified by users and prevent the operator from benefiting from the act’s liability protections, thus placing website operators in the position of requiring authenticated identity information or risk civil liability.

The Defamation Act 2013 was intended to reduce the amount of libel travel that has led to a large number of libel suits with only tenuous connection to the UK being brought in its courts, with relevant sections becoming active in January 2014 that require claimants to prove that England and Wales is the most appropriate forum for the action, set a serious harm threshold for claims, and codify certain defenses such as truth and honest opinion. Such “libel tourism” had a chilling effect on the speech of content producers and ISPs in the UK. However, the number of such claims brought in London increased by 60 percent from 2013 to 2014, resulting in the highest figure since 2009. While the reason for the increase is unclear, one cause could be a number of suits seeking the courts’ clarification of the meaning and scope of the changes to the Act.

In a positive move, new exceptions to copyright protections came into force in October 2014. The

new intellectual property framework included exceptions for making personal copies of protected work for private use, as well as for ‘parody, caricature and pastiche.’\(^{71}\)

**Prosecutions and Detentions for Online Activities**

In what seems to have been the first instance in the UK of a revenge porn prosecution, the Crown Prosecution Service (CPS) charged 21-year-old Luke King for disseminating via social media naked photographs of a woman without her permission and making threats to her.\(^{72}\) The man pleaded guilty and was sentenced in November 2014 to 12 weeks in jail.\(^{73}\)

The Crown Prosecution Service (CPS) had published amended guidelines in October 2014 instructing that the most serious of harassment offenses should be prosecuted under the Sexual Offences Act 2003, carrying a maximum of 14 years in prison where the intent is to coerce the subjects into sexual activity.\(^{74}\) In response to a House of Lords inquiry, the CPS also put forth amended guidelines to clarify the application of its existing social media guidelines to other incidents of revenge pornography, which applied existing laws to such offenses.\(^{75}\)

Prosecutors have also targeted hate speech and incitement to violence based on Islamic extremism. In April 2015, for example, Alaa Esayed, an Iraqi national living in the UK, pleaded guilty to charges of publishing and disseminating terrorist material via Twitter and Instagram from June 2013 to May 2014, resulting in a three-and-a-half year prison sentence.\(^{76}\) While she argued that the content was not hers but rather “cut and pasted” from messages of others, the court held that its dissemination encouraged the recruitment of young people to travel to foreign countries in order to commit terrorist acts.\(^{77}\)

**Surveillance, Privacy, and Anonymity**

Over the past year, several inquiries have studied the UK’s surveillance environment and offered recommendations. In October 2013, the parliamentary Intelligence and Security Committee (ISC) launched an inquiry into the extent and scale of mass surveillance undertaken by Britain’s spy agencies.\(^{78}\) The ISC’s report entitled “Privacy and Security: A modern and transparent legal framework” was released on March 12, 2015, and offered a review of the “intrusive capabilities available to the

---


\(^{73}\) Id.


\(^{75}\) Id.


\(^{78}\) Id.

intelligence agencies.” Although finding that bulk interception does not equate to blanket or indiscriminate surveillance, the report highlighted the tension between rights to individual privacy and collective security. The committee concluded that although the country’s intelligence agencies do not seek to circumvent the law, the complicated nature of the legal framework and the lack of transparency surrounding it mean that current legislation would be better replaced by a new, single act of parliament.

Similarly, a report released in June 2015 from the Independent Reviewer of Terrorism Legislation, David Anderson, called for a clean slate for government surveillance activities, lamenting the fragmentation and obscurity of current laws. A new law should be both comprehensive in scope and comprehensible in nature, the report said.\(^{79}\)

There has been considerable concern over the use of the 2000 Regulation of Investigatory Powers Act (RIPA) with regards to the surveillance of journalists and their sources. Protection of journalistic sources was under heated discussion during 2014-15 following two high profile cases of police accessing journalists’ communication records with the explicit aim of identifying sources, using RIPA to do so. In September 2014, the London-based Bureau for Investigative Journalism filed an application with the European Court of Human Rights to rule on whether UK legislation properly protects journalists’ sources and communications from government scrutiny and mass surveillance.\(^{80}\) The parliamentary Home Affairs Committee’s inquiry into RIPA concluded in December 2014 that RIPA was not fit for purpose and that the legislation governing communications data is in need of complete overhaul.\(^{81}\)

Surveillance has become a major point of contention in the UK following the revelations by Edward Snowden on the activities of GCHQ and its international counterparts, which were published by the Guardian from June 2013 onwards. Garnering the most attention was a secret and extensive surveillance project, codenamed Tempora, that stored the content of communications—phone calls, emails, social networking posts, private messages, and more—for three days, and stored metadata for thirty days, while it was processed by intelligence agents.\(^{82}\) Working with telecom companies, GCHQ installed intercept probes at the British landing points of undersea fiber-optic cables, giving the agency access to some 200 cables by 2012, each carrying a load of up to 10 Gbps of data.

Various legislative measures authorize surveillance,\(^{83}\) including RIPA\(^{84}\) RIPA includes provisions related to the interception of communications; the acquisition of communications data; intrusive surveillance; secret surveillance in the course of specific operations; the use of covert human intelligence sources like agents, informants, and undercover officers; and access to encrypted data. Under current rules, RIPA allows national agencies and over 400 local bodies to access communication records.

---


for a variety of reasons, ranging from national security to tax collection. The 2012 Protection of Freedoms Act imposed new limits on surveillance powers by requiring local authorities to acquire the approval of a magistrate to access communications data.85

A clause within Part I of RIPA supposedly serves as the legal basis for Tempora, allowing the foreign or home secretary to sign off on broad-scale surveillance if communications data is arriving from or departing to foreign soil.86 However, since the UK’s fiber-optic network often routes domestic traffic through international cables, this provision essentially legitimized the GCHQ’s ability to conduct widespread surveillance over most, if not all UK citizens.87

At the same time, the arrangement allows GCHQ to pass on information to its US counterparts in the NSA regarding U.S. citizens, thereby bypassing American restrictions on domestic surveillance. Documents revealed that the U.S. government has provided at least GBP 100 million (US$ 155 million) in funding to GCHQ over the past few years, leading observers to argue that the U.S. government was paying to use information obtained by the UK government.88

In February 2015, the Investigatory Powers Tribunal ruled that the Government Communications Headquarters’ (GCHQ) had acted unlawfully in accessing information collected by its U.S. partner, the National Security Agency (NSA), prior to December 2014. The decision was welcomed by UK-based Privacy International and Pakistan-based Bytes For All, two digital rights organizations that have submitted legal challenges to GCHQ practices. However, they remain in disagreement with an earlier ruling that GCHQ practices after December 2014 were not illegal since they were no longer secret, due to the forceful disclosure of information on the UK-U.S. intelligence relationship. The decision marked the first time the tribunal has ruled against any of Britain’s three intelligence agencies—GCHQ, MI5, and MI6—that it is entrusted to oversee.89

During 2014, 517,236 requests for communications data were submitted by public authorities as a whole (almost 90 percent from police forces and law enforcement agencies), a similar number to the 514,608 received in 2013, while 2,795 lawful intercept warrants were issued, a slight increase from 2760 in 2013.90 Of these, 68 percent were issued for the purpose of tackling serious crime, and 31 percent for national security concerns.

In terms of data protection mechanisms, regulations to implement the 2006 EU Data Retention Directive were adopted in 2009.91 Under the regulations, providers had to retain communications data on all users for 18 months, including mobile phone locations and email logs, known as metadata, but excluding the content of the communications.92 In April 2014, however, the European Court of

92 See The Retention of Communications Data (Code of Practice) Order 2003, accessible: http://www.legislation.gov.uk/
Justice struck down the EU directive as a serious breach of fundamental rights such as privacy.\(^93\) Acting on fears that overseas companies would begin to delete data on UK users, thereby threatening counterterrorism work, the government drew up “emergency” legislation on data retention and placed it on a fast-track through parliament in July 2014.\(^94\) The UK Data Retention and Investigatory Powers Act (DRIPA) requires telecommunication companies to retain users’ metadata for up to 12 months. Shortly after it was passed, academics, journalists, and privacy advocates criticized the legislation for maintaining powers that were struck down by the European court.\(^95\) The new act was framed as a temporary fix and will expire at the end of 2016. At the time of writing, it was being challenged in court by two MPs, David Davis and Tom Watson, represented by human rights group Liberty, arguing that DRIPA is incompatible with both the UK’s Human Rights Act, in particular Article 8, the right to respect for private and family life, and with Articles 7 and 8 of the EU Charter of Fundamental Rights, which call for respect for private and family life and protection of personal data.\(^96\)

There are no public restrictions on the use of encryption technologies. However, under Part 3 of RIPA it is a crime not to disclose an encryption key upon an order from a senior policeman or a High Court judge.\(^97\) The Court of Appeal held in 2008 that such disclosure would not necessarily violate the privilege against self-incrimination.\(^98\) The provision has been used to obtain court orders to force disclosure of keys. Between April 1, 2014 and March 31, 2015, there were 37 court orders for decryption, 29 people charged with refusing to disclose their keys, and 3 convictions for refusal to disclose, with 9 cases still in progress.

Shortly after the terrorist attacks on Paris in January 2015, Prime Minister David Cameron called for a ban on encryption in messaging apps. This was met with criticism from internet freedom and security activists who argued that it would be highly impractical, leaving British communications highly vulnerable,\(^99\) as well as putting an end to e-commerce and introducing excessive filtering.\(^100\) Cameron reaffirmed his commitment to making sure that terrorists were not able to communicate safely via new digital technologies in late June 2015.\(^101\) The UK government plans to put forward a draft investigatory powers bill, dubbed the ‘snoopers’ charter’ by activists, in autumn 2015. It is expected to force tech providers to provide access to encrypted content.

\(^98\) Cory Doctorow, What David Cameron just proposed would endanger every Briton and destroy the IT industry, Boingboing, January 13, 2015, http://boingboing.net/2015/01/13/what-david-cameron-just-propos.html
\(^99\) James Ball, Cameron wants to ban encryption – he can say goodbye to Digital Britain, Guardian, January 13 2015 http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror
\(^100\) Adam Bienkow, David Cameron: Twitter and Facebook privacy is unsustainable http://www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable
United Kingdom

Intimidation and Violence

There were no reported incidences of overt intimidation or violence against users for their online activities over the coverage period.

Technical Attacks

While there have been incidents of cyberattacks in recent years, nongovernmental organizations, media outlets, or activists are not generally targeted by the government or nonstate actors. However, economically motivated fraud and hacking continue to present a challenge to authorities and the private sector.
United States

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>19</td>
<td>19</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 318 million

Internet Penetration 2014: 87 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: No

Bloggers/ICT Users Arrested: No

Press Freedom 2015 Status: Free

Key Developments: June 2014 – May 2015

- In February 2015, the Federal Communications Commission approved new rules that allow it to regulate the internet as a public utility, including provisions to protect net neutrality (see Media, Diversity, and Content Manipulation).

- Members of the government have increasingly called for restrictions on encrypted communications, citing national security and intelligence concerns, while some legislators have taken steps to rebuff these efforts by introducing a bill that would prevent the government from requiring private companies to install encryption “backdoors” (see Surveillance, Privacy, and Anonymity).

- Online journalists and protestors filming police interactions in Ferguson, Missouri, were subject to arrest, intimidation, and harassment by police (see Prosecutions and Detentions for Online Activities and Intimidation and Violence).
United States

Introduction

The United States took a significant step toward protecting the free and open internet in February 2015, when the Federal Communications Commission (FCC) adopted strong, bright-line network neutrality rules, which limit the extent to which internet service providers (ISPs) can pick and choose the content that reaches their subscribers. Net neutrality has dominated internet policy debates in the United States for the better part of a decade, but truly emerged as a subject of widespread public discussion in 2014, after a federal court vacated most of the FCC’s 2010 Open Internet Order in response to a lawsuit led by Verizon, one of the nation’s largest telecommunications companies. Following the court’s January 2014 ruling, thirteen months of vigorous public debate — including the submission of over four million comments1 through the FCC’s online public notice and comment process — culminated in the FCC’s decision to legally classify broadband as a telecommunications service, which in turn enabled it to approve new rules that prohibit blocking and unreasonable discrimination of content on both fixed and wireless networks.2 Those rules are currently in effect, although several broadband companies and their trade associations have sued the FCC in federal court once again to overturn the rules.

Some progress has also been made on important issues like surveillance reform. After months of public advocacy from privacy watchdogs, technology companies, and legal experts, three key sections of the PATRIOT Act expired on June 1, 2015, which prompted Congress to finally pass the USA FREEDOM Act the following day.

At the same time, however, 2015 witnessed the development of some concerning new threats to secure and anonymous speech online. Following major product announcements by Apple and Google in September 2014, a debate emerged between law enforcement officials, technology experts, and privacy advocates about whether companies should be allowed to market products with strong encryption that do not preserve the government’s ability to access decrypted versions of those encrypted communications. High-ranking officials including the FBI Director, the Attorney General, and the Director of the NSA have called on technology companies to find a technical solution to the problem, threatening to seek congressional action if necessary. There have been no actual legislative changes regarding the use of encryption at this time, but the debate has raised serious concerns about the security, free speech, and economic impact if such policies were to be put into place.

Additionally, more reports of police detaining, harassing, and threatening individuals—including professional journalists—for documenting police actions on smartphones or with cameras has called into question the degree to which this right is fully protected. Journalists for online publications were harassed and temporarily detained during demonstrations in Ferguson, Missouri, where people gathered to protest police violence against the black community in the United States.

Obstacles to Access

*Access to the internet in the United States is largely unregulated. It is provided and controlled in practice by a small group of private cable television and telephone companies that own and manage the*

---

1  Gigi B. Sohn and Dr. David A. Bray, “Setting the Record Straight on Open Internet Comments,” Official FCC Blog, Federal Communications Commission, December 23, 2014, [http://fcc.us/1A6hhKs](http://fcc.us/1A6hhKs).
network infrastructure. This model has been questioned by observers who warn that insufficient competition in the ISP market could lead to some increases in the cost of access, thus adversely affecting the economy and individuals’ participation in civic life, which increasingly occurs online. In 2015, however, several important victories for consumers — including the historic net neutrality decision and the collapse of a proposed merger between internet service giants Comcast and Time Warner Cable — suggest that the climate may be improving.

Availability and Ease of Access

Although the United States is one of the most connected countries in the world, the speed, affordability, and availability of its broadband networks has fallen behind several other developed countries. According to the International Telecommunication Union, internet penetration in the United States reached 87 percent by the end of 2014. Broadband adoption rates are high, with approximately 80 percent of Americans subscribing to either a home-based or smartphone-based internet service as of 2013. While the broadband penetration rate is high by global standards, it still puts the United States significantly behind countries such as Switzerland, the Netherlands, Denmark, and South Korea. Moreover, access, cost, and usability remain barriers for many Americans — particularly senior citizens, people who live in rural areas, and low-income households. However, recent data from the Pew Research Center shows that internet access rates for those 65 years of age and older has steadily increased over the past decade, with more 58 percent of individuals in this age bracket using the internet as of 2015.

In January 2015, the Federal Communications Commission (FCC) updated its definition of the term “broadband” to a new benchmark of 25 Megabits per second (Mbps) download and 3 Mbps upload, citing advances in technology, market offerings, and consumer demand. This change is an increase from the previous 4 Mbps download and 1 Mbps upload standard adopted in 2010. Under the new definition, the FCC found that 17 percent of the population lacks access to broadband service. Lack of access is especially prevalent in rural areas, where low population densities make it less appealing for private companies to make large investments in network infrastructure. As a result, less than half of residents in rural areas have access to 25 Mbps broadband service and at least two million Americans still subscribe to dial-up internet in 2015.

Despite a lack of penetration in rural areas, uptake rates for internet-enabled mobile devices have increased dramatically throughout the United States in recent years. In 2014, 90 percent of adults

---

9 Alison Griswold, “2 Million Americans Still Use AOL’s Dial-Up Internet,” Future Tense (blog), Slate, May 13, 2015, http://slate.me/1A0VnxJ.
United States

reported that they own a mobile phone, and 64 percent of adults own a smartphone.\textsuperscript{10} A growing number of people use their phones to check email, visit social-networking sites such as Facebook, and engage in online commerce. This trend has prompted many companies to develop special applications and versions of their websites that are designed for mobile phone viewing. Recent reports by Pew Research indicate that young adults, minorities, and those with lower household incomes are more likely to be “smartphone-dependent,” with limited options for internet access other than their phones.\textsuperscript{11}

Restrictions on Connectivity

Internet users in the United States face few government-imposed restrictions on their ability to access content online. The backbone infrastructure is owned and maintained by private corporations, including AT&T and Verizon. In contrast to countries with only a few connections to the backbone internet infrastructure, the United States has numerous connection points, which would make it nearly impossible to disconnect the entire country from the internet.

At the same time, law enforcement agencies in the United States are known to have and occasionally wield the power to inhibit wireless internet connectivity to respond to emergency situations. The federal government has a non-public protocol for shutting down wireless internet connectivity in response to particular events, some details of which recently came to light following a lawsuit brought under the Freedom of Information Act.\textsuperscript{12} The protocol, known as Standard Operating Procedure (SOP) 303, was secretly established in 2006 on the heels of a 2005 cellular-activated subway bombing in London. SOP 303 codifies the “shutdown and restoration process for use by commercial and private wireless networks during national crisis.” However, what constitutes a “national crisis,” and what safeguards exist against abuse remain largely unknown, as the full SOP 303 documentation has never been released to the public.\textsuperscript{13} State and local law enforcement also have tools to jam wireless internet. For example, in 2011, San Francisco public-transit provider Bay Area Rapid Transit (BART) interrupted wireless service on its platforms to disrupt protests sparked by the police shooting of a homeless man named Charles Hill.\textsuperscript{14} In December 2014, the FCC issued an Enforcement Advisory clarifying that it is illegal to jam cell phone networks without a federal authorization, even for state and local law enforcement agencies.\textsuperscript{15}

ICT Market

There are few obstacles that prevent the existence of diverse business entities providing access to digital technologies in the United States, which is home to a thriving startup community of innovators and entrepreneurs that has produced many low-cost, globally successful online platforms and tools.

\textsuperscript{10} Aaron Smith, Smartphone Use in 2015, Pew Research, \url{http://pewrsr.ch/19JDwMd}.
\textsuperscript{11} Aaron Smith, Smartphone Use in 2015, Pew Research, \url{http://pewrsr.ch/19JDwMd}.
\textsuperscript{12} The Electronic Privacy Information Center (EPIC) filed suit against the Department of Homeland Security (DHS) in 2013 for information about the protocol. After winning an appeal in the DC Circuit, the DHS retained exemption from disclosing SOP 303, and in July of 2015 released a redacted version of the protocol. Electronic Privacy Information Center, EPIC v. DHS – SOP 303, \url{http://bit.ly/1GscPWS}; Electronic Privacy Information Center, SOP 303 Updated Release, \url{http://bit.ly/1W19h3V}.
\textsuperscript{13} Electronic Privacy Information Center, EPIC v. DHS – SOP 303.
\textsuperscript{14} Melissa Bell, “BART San Francisco Cut Cell Services to Avert Protest,” The Washington Post, August 12, 2011, \url{http://wapo.st/1GscX8T}.
\textsuperscript{15} Federal Communications Commission, WARNING: Jammer Use Is Prohibited, December 8, 2014, \url{http://fcc.us/1L1RV2O}.  

875 www.freedomhouse.org
While there are many broadband service providers operating in the United States, the industry has trended toward consolidation. Five dominant providers — Comcast, AT&T, Time Warner Cable, Verizon, and CenturyLink — own the majority of network cables and other infrastructure, serving a combined 65 million customers and controlling 70 percent of the market for 4 Mbps service. For customers subscribing to service that meets the new 25 Mbps benchmark for broadband, the market is even less competitive, with a single provider — Comcast — controlling over 50 percent of the market.

In 2005, the FCC embraced an aggressive deregulation agenda that freed network owners from a longstanding obligation to lease their lines to competing providers. Deregulation proponents claimed that this step would give large cable and telephone companies incentive to expand and upgrade their networks, while opponents worried that the move would lead to higher prices, fewer options for consumers, and worse service. Although average broadband speeds have increased over the past decade, the majority of American households have access to only one broadband provider that offers download speeds of at least 25 Mbps, and nearly 20 percent of Americans have no option at all for internet access at this speed.

Americans increasingly access the internet via mobile technologies, as wireless carriers deploy advanced Long-Term Evolution (LTE) networks. Following a decade of consolidation, the U.S. wireless market is dominated by four national carriers — AT&T, Verizon, Sprint, and T-Mobile — that reach 99 percent of Americans. The U.S. government has looked unfavorably on further consolidation, notably when regulators blocked AT&T’s proposed merger with T-Mobile in 2011 and when regulators signaled that they would block a rumored Sprint/T-Mobile merger in 2014. Moreover, the government promoted the growth of mobile broadband through a series of recent spectrum auctions, including a successful auction in late 2014 and a planned auction in early 2016.

Within the past year, the U.S. government has taken steps to encourage broadband competition. In April 2015, federal regulators at the FCC and the U.S. Department of Justice indicated they would block a proposed merger between Comcast and Time Warner Cable, citing concerns that the combined company would have too much influence over the broadband market. The companies subsequently abandoned the transaction. In January 2015, President Barack Obama announced an initiative to encourage the development of community-based broadband services and asked the FCC to remove barriers to local investment. One month later, the FCC “preempted,” or overturned, state laws in Tennessee and North Carolina that restrict local broadband services, arguing that such laws create barriers to broadband deployment. However, that action is currently being challenged in

23 Federal Communications Commission, “FCC Grants Petitions to Preempt State Laws Restricting Community Broadband in
United States

federal court and similar laws remain valid in many other states.

Regulatory Bodies

No single agency governs the internet in the United States. The Federal Communications Commission (FCC), an independent agency, is charged with regulating radio and television broadcasting, interstate communications, and international telecommunications that originate or terminate in the United States. The FCC has jurisdiction over a number of internet-related issues, especially in light of the February 2015 decision to reclassify broadband as a telecommunications service under the Communications Act. Other government agencies, such as the Commerce Department’s National Telecommunications and Information Administration (NTIA), also play advisory or executive roles with respect to telecommunications, economic and technological policies, and regulations. It is the role of Congress to create laws that govern the internet and delegate regulatory authority. Government agencies such as the FCC and the NTIA must act within the bounds of congressional legislation.

Limits on Content

Access to information on the internet is generally free from government interference in the United States. There is no government-run filtering mechanism affecting content passing over the internet or mobile phone networks. Users with opposing viewpoints engage in vibrant online political discourse and face almost no legal or technical restrictions on their expressive activities online. Additionally, the FCC’s decision in February 2015 to approve net neutrality rules will ensure that ISPs cannot discriminate against traffic based on content. At the same time, recent revelations about the extent of government surveillance of online communications and aggressive investigations into journalists in whistleblower cases have led some to report an increase in self-censorship over the past few years.

Blocking and Filtering

In general, the U.S. government does not block or filter online content. Some states require publicly funded schools and public libraries to install filtering software on their computers to block obscene, illegal, or harmful content. However, the rise of the Islamic State has sparked intense debate about the appropriate role of social media companies in combating the use of mainstream social media as a tool used by terrorist organizations for recruitment and communication. Some government officials say that social media companies are being exploited by terror organizations, and that the companies have an active responsibility to block or remove terror-related content. Various companies maintain their own internal trust and safety policies with regard to hate speech and extremist groups, and in July 2015, the Senate Intelligence Committee approved legislation in a closed hearing that would require “electronic communication service providers” to report suspected terrorist content to federal authorities.

---

United States

Content Removal

Illegal online content—including child pornography and content that infringes on copyright—hosted within the United States can be removed through a court order or similar legal process. However, aside from these examples of illegal content, government pressure on ISPs or content hosts to remove content is not a widespread issue within the United States.

One of the most important protections for online free expression in the United States is Section 230 of the Communications Decency Act (CDA 230), which generally shields online sites and services from legal liability for the activities of their users, thus allowing sites and services with rich user-generated content to flourish. However, although the government does not censor any particular political or social viewpoints, legal rules do restrict certain types of content on the internet, and there have even been some attempts to step back the broad protections of CDA 230. For example, concerns over intellectual property violations, child pornography, protection of minors from harmful or indecent content, harassing or defamatory comments, publication of commercial trade secrets, gambling, and financial crime have presented a strong impetus for aggressive legislative and executive action.

Advertisement, production, distribution, and possession of child pornography—on the internet and in all other media—is prohibited under federal law and can carry a sentence of up to 30 years in prison. According to the Child Protection and Obscenity Enforcement Act of 1988, all producers of sexually explicit material must keep records proving that their models and actors are over 18 years old. In addition to prosecuting individual offenders, the Department of Justice, the Department of Homeland Security, and other law enforcement agencies have asserted their authority to seize the domain name of a website allegedly hosting child abuse images after obtaining a court order.

Congress has passed several laws designed to restrict adult pornography and shield children from harmful or indecent content online, such as the Child Online Protection Act of 1998 (COPA), but these laws have been overturned by courts due to their ambiguity and potential infringements on the First Amendment of the U.S. Constitution, which protects freedom of speech and the press. One law currently in force is the Children’s Internet Protection Act of 2000 (CIPA), which requires public libraries that receive certain federal government subsidies to install filtering software that prevents users from accessing child pornography or visual depictions that are obscene or harmful to minors. Libraries that do not receive the specified subsidies from the federal government are not obliged to comply with CIPA, but more public libraries are seeking federal aid in order to mitigate budget shortfalls. Under the U.S. Supreme Court’s interpretation of the law, adult users can request that the filtering be removed without having to provide a justification. However, not all libraries allow this option, arguing that the decisions about the use of filters should be left to the discretion of individual libraries.

Congress is also considering passing a law known as the SAVE Act, which would help protect against sex trafficking of children by making it a serious criminal offense to knowingly advertise a sex traf-

---

28 Treating domain names as property subject to criminal forfeiture, 18 U.S.C. §2253.
ficking victim, or to benefit from such advertising. A number of civil society groups have pushed back against the proposed law, arguing that the associated harsh penalties would chip away at CDA 230 protections, chill a robust advertising ecosystem that is generally content neutral, and encourage online websites and services to self-censor. As of May 2015, the SAVE Act has passed in the House of Representatives and is under consideration in the U.S. Senate.

The government has in recent years started more aggressively pursuing alleged infringements of intellectual property rights on the internet. Since 2010, the Immigration and Customs Enforcement (ICE) division of the Department of Homeland Security has engaged in several rounds of domain-name seizures, with targets including blogs and file-sharing sites that allegedly link to illegal copies of music and films, as well as sites that sell counterfeit goods. These seizures have been criticized as overly secretive and lacking in due process, Nevertheless, ICE continues to pursue the project, which is known as “Operation In Our Sights.” In December 2013, ICE announced that it partnered with 10 international law enforcement agencies to seize 706 domains allegedly selling counterfeit goods to online consumers. The U.S. component of this initiative resulted in the seizure of 297 domains. In December 2014, the partnership announced the seizure of an additional 292 domains, bringing the total number of seizures so far to 1,829.

Not only is the ICE now involved in interfering with online content that implicates intellectual property rights, but last year the International Trade Commission (ITC), a trade agency that can block the importation of articles that infringe intellectual property, joined the fray. The ITC normally deals with the importation of physical articles, but in an unprecedented move in 2014, the ITC declared that it had the authority to block the cross-border transmission of data violating a U.S. patent. In a letter to the ITC, a number of civil society groups and academic scholars urged the ITC to reconsider its stance that it can block pure data transmissions, cautioning that the “decision has enormous ramifications, opening the door to internet content blocking efforts rejected by Congress and the public.” The ITC paused on action pending a Federal Circuit ruling on the case.

For copyright infringement claims, the removal of online content is dictated by the safe harbor provisions created in Section 512 of the Digital Millennium Copyright Act (DMCA). Operating through a “notice-and-takedown” mechanism, ISPs are shielded from liability if they remove infringing content upon receipt of a DMCA notice. However, because ISPs have the incentive to err on the side of caution and remove any hosted content subject to a DMCA notice, there have been occasions where overly broad or fraudulent DMCA claims have resulted in the removal of content that would otherwise be excused under free expression, fair-use, or educational provisions.

In recent years, a number of internet companies have taken to publicly reporting requests to remove content. Many of these reports focus on trademark-related requests or requests alleging copyright infringement under the DMCA. There is also some concern regarding the intellectual property sections of the Trans-Pacific Partnership, and whether the proposed trade agreement would extend portions of U.S. copyright terms internationally.\textsuperscript{41}

In 2012, Google started reporting information about the copyright removal notices it receives, including how often notices are received, the names of the copyright owners or their agents who submit the requests, and the websites identified.\textsuperscript{42} The company also reports on how often infringing links are removed from search results. A number of other major internet companies, including Twitter, Automattic (publisher of Wordpress.com), and the Wikimedia Foundation, similarly report on intellectual property takedowns. Companies have also expanded their practices to include their compliance rates and, in some cases, information about the links or content the company did not remove because it was deemed non-infringing. Transparency around unactionable DMCA claims may become increasingly popular in light of the number of abuses of the copyright takedown system.

While reporting on copyright removal requests is growing, so too is the practice of reporting on government requests to remove content. Major internet companies, including Twitter, Facebook, Yahoo, and Pinterest, publicly share information about these requests, which come from around the world. According to Twitter, “[g]overnments generally make removal requests for content that may be illegal in their respective jurisdictions,” such as hate speech, defamatory statements, or child pornography.\textsuperscript{43} According to the latest data publicly released by Twitter, between July and December of 2014, the social media company received 6 court orders and 26 U.S. government requests to remove or withhold content, although the company also reported zero percent compliance for the 32 requests.\textsuperscript{44} In 2014, Yahoo received 5 U.S. government removal requests for a total of 11 items and complied with 4 of the 5 requests. The company reports that it did not comply with “a court order from a U.S. government agency to remove content” because the company “did not host any of the domains or content.”\textsuperscript{45}

### Media, Diversity, and Content Manipulation

The online environment in the United States is vibrant, diverse, and generally free of economic or political constraints. Anyone can start a blog, forum, or social media site to discuss opinions and share news and information. Due to the FCC’s decision to protect net neutrality regulations, ISPs cannot throttle, block or otherwise discriminate against internet traffic based on its content. Self-censorship, however, continues to exist to some degree due to the extensive government surveillance revealed over the past two years.

The concept of network neutrality — a foundational principle of the internet that prohibits network operators from giving preferential treatment to favored content or from blocking disfavored content — has dominated internet policy debates in the United States for the better part of a decade. The issue emerged in the early 2000s and gained widespread attention in 2008 when the FCC penalized


\textsuperscript{44} Ibid.

Comcast, a major American broadband provider, for throttling a file-sharing application called BitTorrent. A federal court later overturned the FCC’s action against Comcast on procedural grounds, prompting the FCC to initiate a formal rulemaking process to codify network neutrality principles in U.S. law. The result was the 2010 Open Internet Order, a series of rules protecting lawful online content from blocking or unreasonable discrimination. A federal court vacated most of the 2010 rules in January 2014 in response to a lawsuit led by Verizon, one of the nation’s largest telecommunications companies. The court held that the FCC had based the order on insufficient legal authority, eliminating the United States’ only legal protections for network neutrality.

The success of Verizon’s lawsuit sparked a public campaign for new rules that lasted more than a year and drew support from President Barack Obama, members of Congress, technology companies, consumer advocates, and millions of Americans who contacted the FCC. In February 2015, the FCC approved a new Open Internet Order that many legal experts believe is based on stronger legal authority than the 2010 order. The order prohibits blocking and unreasonable discrimination on both fixed and wireless networks, reflecting the growing importance of mobile broadband in the United States. However, several broadband companies and their trade associations are once again suing the FCC to overturn the rules. As of May 2015, the lawsuit was pending in federal court and many technology companies and public interest groups had formally joined the case to oppose the lawsuit and defend the FCC’s rules.

Although the U.S. Constitution includes core protections for freedom of the press, the U.S. government does bring some enforcement actions against whistleblowers and journalists that may lead to self-censorship. The Attorney General has said that the government would not prosecute Glenn Greenwald, the journalist who first published documents leaked by Edward Snowden, or “any journalist who’s engaged in true journalistic activities,” but investigations and prosecutions of several other whistleblowers and journalists are ongoing. In addition to the ongoing WikiLeaks grand jury investigation, which targeted at least three journalists’ Google email accounts and metadata, reporters from several major media outlets have had their communications collected in pursuit of other whistleblower investigations. As part of one investigation, for example, Fox News correspondent James Rosen was listed as a co-conspirator, was the subject of a warrant for his personal emails, and had his phone calls and appointments with a State Department suspect monitored. In a separate investigation, the Department of Justice obtained two months’ worth of Associated Press journalists’

---

52 Sari Horowitz, “Justice is reviewing criminal cases that used surveillance evidence gathered under FISA,” Washington Post, November 15, 2013, http://wapo.st/1lKgo5Z.
United States

phone records. In July 2013, in response to serious concerns raised by these investigations, the Department of Justice tightened the rules governing when and how the government could access journalists’ records in investigations to ensure journalists could no longer be listed as co-conspirators, and to make it more difficult to obtain journalists’ records without advance notice. In October 2014, Attorney General Eric Holder also acknowledged that the investigation into Rosen was his greatest regret.

Until January 2015, James Risen, an investigative reporter with the New York Times, was involved in an investigation into a whistleblower who was a source of information for his 2006 book, State of War. At some point between 2008 and 2015, Risen’s phone and email records were collected, and he faced possible imprisonment for refusing to disclose the name of his source. In 2015, the government relented and announced that it would not force Risen to testify about his source.

Despite some improved protections, journalists report that their ability to investigate and publish freely is chilled. Several recent studies have concluded that the aggressiveness with which the Department of Justice investigates leaks — as well as pervasive government surveillance programs such as those disclosed by Edward Snowden — causes journalists and writers to self-censor and raises concerns about whether they are able to protect the confidentiality of their sources.

In January 2015, the free expression and literature advocacy group PEN America released the results of an updated survey showing that the NSA surveillance revelations and other government actions had resulted in increased self-censorship among writers. During the 2014 year, 42 percent of respondents reported having altered or avoided social media activities, 31 percent reported deliberately avoiding certain topics in phone or email conversations, and 34 percent reported avoiding writing or speaking about a particular topic. Additionally, Human Rights Watch and the American Civil Liberties Union conducted a survey of journalists and lawyers revealing the degree to which surveillance has impacted their ability to communicate with sources and clients confidentially. Journalists reported that government officials are significantly less likely to speak with journalists than they were a few years ago due to concerns about anonymity and the ability of the intelligence agencies to access their communications information. Lawyers also reported facing increasing pressure to conceal or secure their communications with clients, particularly in cases with foreign governments or prosecutions that might spark an intelligence inquiry.

62 Human Rights Watch and American Civil Liberties Union, With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy.
United States

New evidence suggests that even ordinary American citizens are changing their behavior because of extensive government surveillance. A March 2015 study by the Pew Research Center on Americans’ privacy strategies post-Snowden noted that 30 percent of people surveyed had altered their behavior including changing privacy settings, being more selective about applications they use, or communicating in person instead of online or over the phone.63

Digital Activism

Political activity in the United States is increasingly moving online. According to a 2014 survey by the Pew Research Center, between the 2010 and 2014 midterm elections, the proportion of Americans using social media to follow politicians more than doubled, from 6 percent to 16 percent.64 In 2013, another Pew survey found that 34 percent of American adults used online methods to contact a government official or to speak out in a public forum; 39 percent participated in political activity using a social networking site like Facebook or Twitter in the prior year; and 21 percent of email users reported regularly receiving calls to action on social or political issues by email.65 In addition, political candidates and elected officials increasingly use email, mobile apps, and online content to garner support and keep their constituents engaged. Researchers have come to a general consensus that internet use is now deeply linked to political participation and citizenship.66

An unprecedented number of Americans used online tools to mobilize in support of the open internet in 2014, resulting in the FCC’s passage of a historic network neutrality order. Nearly 4 million Americans contacted the FCC about its proposed net neutrality rules — a record-breaking number that far exceeded the number of comments the agency had received on any topic in its history.67 The FCC’s website crashed several times as a result of the influx of public comments, notably after comedian John Oliver urged Americans to contact the agency in a televised rant that went viral on social networking websites.68 A broad coalition of grassroots organizations, advocacy groups, and technology companies used online tools to mobilize supporters and pressure the FCC and elected officials. In September 2014, members of this coalition staged an “Internet Slowdown Day” in which dozens of high-profile websites displayed a spinning wheel to indicate what the internet could look like in a world without net neutrality protections.69 When the FCC approved the strongest network neutrality rules in its history in February 2015, policymakers credited the millions of Americans who spoke out in online forums.70

---

63 Lee Rainieand and Mary Madden, Americans’ Privacy Strategies Post-Snowden, Pew Research Center, March 16, 2015, http://pewrsr.ch/1MhtHwJ.
68 Soraya Nadia MacDonald, “John Oliver’s net neutrality rant may have caused the FCC website to crash,” Washington Post, June 4, 2014, http://wapo.st/1mrTd8J.
United States

Violations of User Rights

The United States has a robust legal framework that supports freedom of expression both online and offline, and the state does not typically prosecute individuals for online speech. The broader picture of user rights in America, however, has become increasingly complex as a series of U.S. government practices, policies, and laws touch on, and in some cases appear to violate, the rights of individuals both inside the United States and abroad. Government surveillance is a major concern, especially following revelations about NSA practices. Aggressive prosecution under the Computer Fraud and Abuse Act (CFAA) has also been criticized. In addition, the privacy of NGOs, companies, and individual users is threatened by a growing number of cyberattacks initiated by both domestic and international actors.

Legal Environment

The First Amendment of the U.S. Constitution includes protections for free speech and freedom of the press, and in 1997 the US Supreme Court reaffirmed that online speech has the highest level of constitutional protection. Lower courts have consistently struck down attempts to regulate online content. Two federal laws also provide significant protections for online speech: Section 230 of the Communications Act of 1934 (as amended by the Telecommunications Act of 1996) provides immunity for ISPs and online platforms such as YouTube and Facebook that carry content created by third parties. The Digital Millennium Copyright Act (DMCA) of 1998 provides a safe harbor to intermediaries that take down allegedly infringing material after notice from the copyright owner. These statutes enable companies to develop internet applications and websites without fear that they will be held liable for content posted by users.

There are some concerns, however, over conflicts about the right to remain anonymous in online communications, which often arise in cases of hate speech, defamation or libel. For example, in a recent case before the Supreme Court of Virginia, a judge ruled that a Virginia court could not compel Yelp to reveal the identities of anonymous users.

Complementing these legal protections, a number of U.S. laws attempt to protect speech from harmful corporate actions as well, including corporate surveillance that may lead users to self-censor, and failure of private actors to sufficiently protect internet users’ personal information from unauthorized access. Section 5 of the Federal Trade Commission Act (FTCA) has been interpreted to prohibit entities operating over the internet from deceiving users about what personal information is being collected and how it is being used, as well as from using personal information in ways that harm users without offering countervailing benefits. In addition, the FTCA has been interpreted to require entities that collect users’ personal information to adopt reasonable security measures to safeguard it from unauthorized access. State-level laws in 47 U.S. states and the District of Columbia also require entities that collect personal information to notify consumers—and, usually, consumer protection agencies—when they suffer a security breach leading to unauthorized access of personal information. Section 222 of the Communications Act prohibits telecommunications carriers from

---

73 Justin Jouvenal, “Yelp won’t have to turn over names of anonymous users after court ruling” Washington Post, 16 April 2015, [http://wapo.st/1MbcE48](http://wapo.st/1MbcE48)
sharing or using information about their customers’ use of the service for other purposes without customer consent. This provision has historically only applied to phone companies’ records about phone customers, but following the FCC’s net neutrality order, it now also applies to ISPs’ records about broadband customers.

**Prosecutions and Detentions for Online Activities**

In the aftermath of the police killings of Eric Garner, Freddie Gray, and Michael Brown in New York, Baltimore, and Ferguson respectively, several citizen journalists were arrested or reported police intimidation while attempting to record police activity with smartphones. The right of civilians to film or record the police is protected under the First Amendment; however, during the Ferguson protests at least 21 journalists were arrested, including reporters for the *Huffington Post* and the *Washington Post*. In addition, St. Louis Alderman Antonio French was detained by the police while covering police activity through live-tweets; French had also been uploading short videos and images to the social media platforms Vine and Instagram.

Aggressive prosecution under the Computer Fraud and Abuse Act (CFAA) has fueled growing criticism of that law’s scope and application. Under CFAA, it is illegal to access a computer without authorization, but the law fails to define the term “without authorization,” leaving the provision open to interpretation in the courts. In one prominent case, programmer and internet activist Aaron Swartz secretly used Massachusetts Institute of Technology servers to download millions of files from a service providing academic articles. Prosecutors sought harsh penalties for Swartz under CFAA, which could have resulted in up to 35 years imprisonment. Swartz committed suicide in early 2013. Shortly after his death, a bipartisan group of lawmakers introduced “Aaron’s Law,” draft legislation that would prevent the government from using CFAA to prosecute terms of service violations and stop prosecutors from bringing multiple redundant charges for a single crime. The bill was reintroduced in 2015, but has not garnered enough support to move forward. Meanwhile and in contrast to Aaron’s Law, the Obama Administration—rather than supporting CFAA reform—has instead proposed draft legislation that would broaden the scope of activities covered under CFAA and make its penalties even harsher.

Many states also have their own laws related to computer hacking or unauthorized access. Several smaller cases in the past year highlight the shortcomings and lack of proportionality of these laws. In December 2014, a 21-year-old Georgia Tech student named Ryan Gregory Pickren was arrested on felony computer trespass charges after hacking into the University of Georgia’s online calendar as part of a prank leading up to a football game. The prank calendar post, which was titled “Get Ass Kicked by GT,” was live for approximately an hour before it was discovered and removed. However, according to Georgia state law, a person convicted for computer trespass—defined as “alter[ing], damag[ing] or in any way caus[ing] the malfunction of a computer, computer network, or computer

---

program regardless of how long it occurs”—faces a maximum penalty of 15 years in prison and a $50,000 fine.\(^8\) Pickren was ultimately accepted into a pretrial intervention program, and his charges will be dismissed upon his satisfactory completion. Similarly, in early 2015, Florida authorities arrested a 14-year-old middle school student named Domanik Green on felony cybercrime charges after the boy used a teacher’s administrative password to log onto a school computer and change its desktop background.\(^8\)

### Surveillance, Privacy, and Anonymity

Concerns over government surveillance have grown since Edward Snowden’s June 2013 revelations about NSA access to domestic and foreign communications. In response, Congress has put forth multiple legislative proposals to restrict, or in some cases maintain, NSA surveillance capabilities over the past two years. In January 2014, President Obama announced that he intended to end the bulk collection of telephony metadata.\(^8\) In January 2015, the president also issued updates to the administration’s 2014 policy directive that put in place important new restrictions on the use of information collected in bulk for foreign intelligence purposes.\(^8\)

Additionally, in December 2014, Congress passed a bill that included a requirement that the NSA develop “procedures for the retention of incidentally acquired communications” collected pursuant to Executive Order 12333, and that, except when subject to certain broad exceptions, those communications may not be retained for more than five years.\(^8\) This is the first time that Congress has legislated on executive activities under Executive Order 12333.

In June 2015, Congress passed the USA FREEDOM Act to extend expiring provisions of the PATRIOT Act, but with significant reforms to PATRIOT Act Section 215, as well as to the FISA Pen Register and Trap and Trace Device and National Security Letters authorities, both of which were also used for bulk or large-scale collection of Americans’ information. The USA FREEDOM Act was broadly supported by the Attorney General, the Director of National Intelligence, Democrats and Republicans in Congress, as well as civil society and the private sector. Despite this broad support, it took several months to pass the act, and the final version embodied weaker reforms than what was advocated for by many supporters of surveillance reform. Owing to the difficulty of getting reform through Congress, reauthorization did not occur before a number of PATRIOT Act provisions expired on June 1, 2015.\(^8\) After a single day lapse in surveillance authority, Congress finally passed the USA FREEDOM Act, and President Obama signed it into law the same night.\(^8\) The USA FREEDOM Act marks the most significant reforms to U.S. surveillance law since the Patriot Act passed in 2001.

Prior to the passage of the USA FREEDOM Act, as Congress was still debating legislative reforms, the

---

81 Josh Solomon, “Middle school student charged with cybercrime in Holiday,” [Tampa Bay Times](http://bit.ly/1v6qTRq), April 9, 2015.
82 The White House, Office of the Press Secretary, “Remarks by the President on Review of Signals Intelligence,” January 17, 2014, [http://1.usa.gov/1LoeITT](http://1.usa.gov/1LoeITT).
United States
courts considered three cases challenging the legality and constitutionality of the NSA’s bulk collection program under PATRIOT ACT Section 215. In May 2015, the Second Circuit Court of Appeals ruled that the program was illegal, and that the government’s interpretation of the term “relevance” exceeded what was authorized by statute. The court did not comment on the constitutional questions raised by bulk collection.87 Two other cases are still pending, and the issue may eventually be taken up by the Supreme Court.

Finally, in April 2015, it was revealed that since the 1980s, the Department of Justice and the Drug Enforcement Agency had been collecting Americans’ phone record metadata in bulk, amassing billions of records, apparently using the same interpretation of the term “relevance” that was the basis for the bulk collection program under PATRIOT Act Section 215. The program was stopped by Attorney General Eric Holder in September 2013, in response to the Snowden leaks which began earlier that summer.88 Privacy, civil rights, and human rights organizations have spoken out in strong opposition to the program. The day the collection became public, Human Rights Watch filed a legal challenge to the program seeking that it be declared unlawful.89

Although some of the most popular social media platforms in the United States require users to register and create accounts using their real names through Terms of Service or other contracts,90 there are no legal restrictions on user anonymity on the internet. Constitutional precedents protect the right to anonymous speech in many contexts. There are also state laws that stipulate journalists’ right to withhold the identities of anonymous sources, and at least one such law has been found to apply to bloggers.91 In April 2011, the Obama administration launched the National Strategy for Trusted Identities in Cyberspace (NSTIC). The stated goal of the effort is to support the creation of an “identity ecosystem” in which internet users and organizations can more completely trust one another’s identities and systems when carrying out online transactions requiring assurance of identity.92 The plan specifically endorses anonymous online speech.93

While there are no legal restrictions on anonymous communication online, there are concerns about cases in which law enforcement has required social media companies to turn over user information to support an investigation, and forbidden the companies from disclosing any information about the subpoena to impacted users. There is also evidence to suggest that the intelligence community in the United States has been working to undermine the security of anonymizing tools.94 Documents leaked by Edward Snowden suggest that the NSA may have been engaged in cyberattacks, including a project to develop malware targeting users of Tor (a tool that enables people to communicate anonymously online),95 as well as efforts to undermine international technical standards for encrypt-

89 David Ingram, “Rights group sues DEA over bulk collection of phone records,” Reuters, April 8, 2015, http://reut.rs/1E7A0bj.
94 For an in-depth discussion of NSA efforts to undermine internet security, including attacks on Tor (a popular service used to anonymize web traffic) and attempts to undermine international encryption standards through the “Costs to Cybersecurity” in Danielle Kehl et al., “Surveillance Costs: The NSAs Impact on the Economy, Internet Freedom, and Cybersecurity,” New America’s Open Technology Institute, July 2014, http://bit.ly/1Gsr5BD.
95 James Ball, Bruce Schneier and Glenn Greenwald, “NSA and GCHQ Target Tor Network that Protects Anonymity of Web
United States

tion. Moreover, as major technology companies have begun enhancing their use of encryption technology in the past year, it has reignited a debate between law enforcement officials, technology experts, and privacy advocates about whether companies should be allowed to market products with strong encryption that do not preserve the government’s ability to access decrypted versions of those encrypted communications.

In September 2014, Apple announced that it would be moving to smartphone encryption by default on all devices running its new iOS, followed a few days later by a similar announcement from Google about the latest version of the Android operating system. In addition to advances in hardware encryption, a number of companies took greater steps to make end-to-end encryption available for email and messaging services, including the popular mobile messaging service Whatsapp and a joint Google-Yahoo effort to develop an easy-to-use encryption browser extension for their email services. The added protection is, at least in part, a reaction to diminishing trust in American technology products following the 2013 Snowden leaks and increasing pressure from advocacy groups, individuals, and customers who are concerned about the security of their data. In the year after the Snowden disclosures, encrypted web traffic doubled in North America.

However, the Apple and Google announcements in particular have prompted serious backlash from the law enforcement and intelligence communities in the United States. The FBI Director has argued that Apple’s and Google’s new privacy-enhancing features will “allow people to place themselves beyond the law” and that default encryption could seriously hinder criminal investigations, calling on Congress to take action to force companies to maintain some kind of backdoor to allow government access to communications if a warrant has been obtained. The Manhattan District Attorney called device encryption a threat to public safety, while the former Attorney General urged tech companies to leave backdoors open for police. Their arguments have received support from the National Security Agency and the Office of the Director for National Intelligence as well. In the subsequent


months, there has been a great deal of debate about the technical feasibility of implementing surveillance backdoors without undermining the overall security of cryptographic systems.104

On the other side of the spectrum, there have been efforts to codify rules that would bar the government from requiring surveillance backdoors. In the summer of 2014, the U.S. House of Representatives approved, with overwhelming bipartisan support, an appropriations amendment to ban spending on government-mandated backdoors, although procedural maneuvers prevented it from being adopted into the final bill.105 In the summer of 2015, the House again approved two similar amendments.106 Building on that support, the Secure Data Act was introduced in Congress in December 2014, which would similarly prohibit the government from requiring that companies weaken the security of their products or insert backdoors to facilitate access.107

Despite a vigorous debate, there have been no actual changes on the legislative front regarding the use of encryption, nor is there any indication that the government is currently planning to move forward with the technical solutions it has proposed.108 While the Communications Assistance for Law Enforcement Act (CALEA) currently requires telephone companies, broadband carriers, and interconnected Voice over Internet Protocol (VoIP) providers to design their systems so that communications can be easily intercepted when government agencies have the legal authority to do so, it does not cover online communications tools such as Gmail, Skype, and Facebook.109 Calls to update CALEA to cover online applications and communications have not been successful. In May 2013, a group of 20 technical experts published a paper explaining why such a proposal (known as “CALEA II”) would create significant internet security risks.110

Since the June 2013 surveillance revelations, internet and telecommunications companies have increasingly taken up the practice of “transparency reporting” in an effort to shed light on the government’s surveillance powers and how the companies handle requests. Transparency reports, which are voluntarily published, detail requests for government access to user information, user communications, and/or requests to have content removed or filtered. One limit to the reporting, however, has been the U.S. Department of Justice’s restrictions on disclosure of information about national security orders.111 In October 2014, Twitter filed suit against the DOJ, arguing that the government’s restrictions on what information companies can disclose about national security letters are unconsti-

---


107 Secure Data Act of 2014, S.2981, 113th Cong. (2014), http://1.usa.gov/1Lc1EmE. The bill was reintroduced in 2015, although no further action has been taken.


tutional.112 Earlier in 2014, the Justice Department had reached a settlement with Facebook, Google, LinkedIn, Microsoft, and Yahoo that would permit the companies to disclose the number of government requests they receive – but only in aggregated bands of 0-249 or 0-999.113 Twitter, not a party to the settlement, has refused to publish data in these aggregated bands because the company believes the DOJ rules amount to an unconstitutional prior restraint that violates the company’s First Amendment rights.114 The DOJ has called for dismissal of the lawsuit.115 A large and wide-ranging group of internet and telecommunications companies, including Wikipedia and Automattic (publisher of Wordpress.com), have shown support for Twitter’s challenge to the DOJ rules by filing briefs in court in support of Twitter.116

The U.S. District Court for the Northern District of California may no longer proceed with the lawsuit, however, given new legal processes implemented by the USA FREEDOM Act.117 Under the new law, companies now have several options on how to report the number and nature of national security orders and other government requests, and can also do so in a more granular fashion than was previously permitted. Yet, depending on the option, these reports are still subject to time delays and have limitations on the frequency of reporting.118

In addition to monitoring private communications, law enforcement agencies have also used open, public websites and social media platforms to monitor different groups for suspected criminal activity. The New York Police Department (NYPD) is one such agency, with the Associated Press reporting that, from 2006 onward, the NYPD Cyber Intelligence unit monitored blogs, websites, and online forums of Muslim student groups and produced a series of secret “Muslim Student Association” reports describing group activities, religious instruction, and the frequency of prayer by the groups.119 Muslim students from across the nation expressed concern about this type of surveillance and told Freedom House that they often self-censor when conducting online activities. In April 2014, the NYPD closed down one unit that monitored locations associated with the Muslim community, including mosques and businesses.120 Civil liberties advocates welcomed this step but warned that other NYPD units may still be using discriminatory practices.

Federal intelligence agencies closely monitor social media as part of their terrorism investigations.121 This monitoring leads to the identification of specific targets, who are then contacted by FBI informants. This was the case in the January 2014 arrest of an Ohio man whose posts on Twitter first drew

117 Dan Levine, “UPDATE 1-Judge casts doubt on Twitter lawsuit over surveillance,” Reuters, June 11, 2015, http://reut.rs/1V8u4MI.
the attention of the FBI and who was ultimately arrested for planning to attack the Capitol.\textsuperscript{122} While monitoring open, public websites and social media platforms has yielded some arrests, it is not limited to targets of investigations, but rather is used to identify targets, and includes monitoring of innocent individuals’ online activities. Thus, it may chill online speech.

In comparison to real-time communications, the status of stored communications is more uncertain. One federal appeals court has ruled that the Constitution applies to stored communications, so that a judicial warrant is required for government access.\textsuperscript{123} However, the 1986 Electronic Communications Privacy Act (ECPA) states that the government can obtain access to email or other documents stored in the cloud with a mere subpoena issued by a prosecutor or investigator without judicial approval.\textsuperscript{124} Bills to update ECPA have had significant support, including from the White House, but have thus far failed to pass. As of mid-2015, advocates continue to push for reform to ECPA that would require government officials to obtain a warrant before compelling online service providers to disclose private communications, including email and documents stored using cloud services.\textsuperscript{125}

**Intimidation and Violence**

In addition to arrests and detentions for filming police activities, individuals have been subject to intimidation and harassment. Kevin Moore, the man who used his cellphone to capture and upload footage of Freddie Gray's arrest by the Baltimore police to YouTube, was also detained by the police after releasing the video. Additionally, Moore claims he was followed by the police and experienced other forms of intimidation.\textsuperscript{126} Similarly, Ramsey Orta, the man who filmed the fatal arrest of Eric Garner by the NYPD—footage in which Garner repeatedly states “I can't breathe” after being placed in a chokehold—also claims to have been repeatedly followed, harassed, and intimidated by the police after his role in documenting the killing. Since the footage was released, the 23-year old Orta has been arrested on three separate occasions and currently awaits trial for multiple charges.\textsuperscript{127}

**Technical Attacks**

Financial, commercial, and governmental entities in the United States are targets of significant cyberattacks. Government policies and laws are in place to prevent and protect against cyberattacks, though many question their impact, effectiveness, and respect for civil liberties.

In August 2014, reports revealed that JPMorgan Chase and several other major U.S. financial institutions were hit with a cyberattack that “funneled off gigabytes of data.”\textsuperscript{128} Similar attacks were carried out against the retailers eBay and Home Depot in 2014. In addition to the attacks resulting in data theft, U.S. banks fell victim to the “Carbanak” cyber-heist that siphoned nearly $1 billion from finan-

\textsuperscript{123} United States v. Warshak, 09-3176, United States Court of Appeals for the Sixth Circuit.
\textsuperscript{124} Ibid.
\textsuperscript{128} Laura Lorenzetti, “JPMorgan Chase, other U.S. banks hit by cyberattacks,” Fortune, August 28, 2014, http://for.tn/1j0scQV
United States

cial institutions since 2013. Finally a high-profile attack on Sony Pictures Entertainment’s internal networks extracted private data and leaked it to the public. The attack on Sony Pictures was likely politically driven, as the attackers attempted to blackmail the company with the stolen data to prevent it from releasing a controversial comedy about North Korea.

Financial and commercial institutions are not the only U.S. institutions subject to cyberattacks. Health information has been the target of a number of high profile attacks, and a reported 90 percent of healthcare providers experienced a breach in the past two years. The motive for breaches of health records is usually financial, as those records can in turn be used to facilitate medical identity theft. There has been some speculation that some of these attacks may be the work of foreign state-sponsored hackers looking to uncover information about defense contractors, government employees, and others with close ties to the U.S. government.

The defense sector and federal government are also frequently under attack. In April 2015, the public learned that Russian hackers had breached the White House’s system, accessing the email archives of President Obama and other sensitive information, including real-time, non-public details of the president’s schedule. In June 2015, news broke that hackers had breached the U.S. Office of Personnel Management’s records system, affecting the records of 4.1 million current and former federal employees. The breach was linked to a Chinese state-backed hacker known as “Deep Panda.” In response to these incidents and others, the U.S. has begun to take legal and policy measures to address growing cyber-threats.

In particular, the U.S. Congress has been attempting to pass a law to facilitate greater sharing of information about cyber-threats. As of June 2015, Congress was considering the Cyber Information Sharing Act of 2015 (CISA). Civil liberties advocates have heavily criticized the bill, in particular contending that it authorizes too much information sharing between companies and the government, allows companies to monitor all of their users’ activities and communications, does not adequately restrict use of CISA-derived information, has poor liability protections for consumers, and authorizes companies to employ potentially dangerous counter-measures when hacked. As of June 2015, Congress was also considering a number of legislative proposals to mandate security protections for personal information held by private entities.

In addition to the legislative activity, President Obama has issued two Executive Orders aimed at addressing cyberattacks. In January 2015, in response to the Sony Pictures hack, Obama issued an order authorizing the Treasury Department to impose sanctions on individuals and entities associated with the North Korean government. Then, in April, the White House issued an Executive Order

permitting the U.S. Department of the Treasury to levy sanctions against individuals or companies that conduct "significant malicious cyber-enabled activities."\(^{137}\)

Law enforcement has also played a role in creating a framework to deter cyberattacks. In May 2014, the Western District of Pennsylvania indicted six officers in Unit 61398 of the Third Department of China's People's Liberation Army (PLA), alleging economic espionage against a number of U.S. based companies.\(^{138}\) In July 2014, the Department of Justice announced that it charged Su Bin, a Chinese businessman, with hacking the computers of “Boeing, Lockheed Martin, and other aerospace companies” with the intent to gather data on the F-22, F-35, and C-17 aircrafts.\(^{139}\)

---


Uzbekistan

Internet Freedom Status

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>Not Free</td>
<td>Not Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>20</td>
<td>19</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>31</td>
<td>31</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>79</td>
<td>78</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

| Population: | 30.7 million |
| Internet Penetration 2014: | 44 percent |
| Social Media/ICT Apps Blocked: | Yes |
| Political/Social Content Blocked: | Yes |
| Bloggers/ICT Users Arrested: | Yes |
| Press Freedom 2015 Status: | Not Free |

Key Developments: June 2014 – May 2015

- Internet access continued to improve slightly during the coverage period, with the internet penetration rate increasing to 43 percent by the end of 2014 (see Availability and Ease of Access).

- A new regulatory body has consolidated state regulation of ICTs, including regulation of access to the internet and online content dissemination (see Regulatory Bodies).

- Amendments to the Law on Informatization in September 2014 established legal liability for bloggers and included requirements that they only report verified information (see Content Removal).

- After 10 years of reporting, the independent news website Uznews closed down after hackers leaked confidential information revealing the identities of some of its reporters, putting those individuals at risk of government’s retaliation for their critical reporting (see Intimidation and Violence).
Uzbekistan

Introduction

Uzbekistan has one of the most tightly controlled online and media environments in the world, with restrictions on any content critical of the government, high levels of surveillance, and prosecutions with lengthy prison sentences for posting controversial content online. Internet freedom registered few improvements during the coverage period of this report, which included the presidential elections on March 29, 2015 and parliamentary elections in December 2014. These political events may have influenced the adoption of legislative amendments targeting bloggers in September 2014. Viewed by many as a further attempt to curb any critical viewpoints and discourage news-oriented blogging, the new amendments force bloggers and other website or webpage owners to conform to stringent content regulations that previously applied only to professional journalists. Penalties for noncompliance include “limited access” to bloggers’ websites and liability under the law, possibly including house arrest, a sanction introduced by the legislators in the same period as blogger regulation.

Obstacles to Access

Access to the internet continues to improve slightly, due to an increase in internet and mobile phone penetration rates. However, internet access is still mainly concentrated in a few large cities, and prices remain prohibitive for the majority of the population.

Availability and Ease of Access

According to data from the International Telecommunication Union (ITU), the internet penetration rate in Uzbekistan reached 43 percent by the end of 2014, compared to 38 percent in 2013 and just 17 percent in 2009.¹ Digital divides exist between the capital of Tashkent and the country’s 12 regions (viloyati) as well as across urban, rural, and remote areas. Tashkent has the highest internet penetration rate and is a nationwide leader in terms of FTTB and WiMAX broadband connectivity.² The lowest internet penetration rate is in the semi-autonomous republic of Karakalpakstan, home to the Karakalpak, Kazakh, and Uzbek ethnic groups.³ The usefulness of ICTs, especially in rural and remote areas, still depends on a stable electricity supply to the telecommunications infrastructure.⁴ Factors including computer skills, household income, and availability of a computer in one’s household continue to determine how often individuals use the internet.

Internet access is based primarily on the use of ADSL connections. According to the latest ITU data, a mere 389,000 internet users had a fixed-broadband subscription in 2014.⁵ The construction of the fiber-optic network (FTTx) in Uzbekistan required US$9 million in Uzbek and Chinese investments.

---

Uzbekistan

from 2013–2014.6 By January 2014, the fibre-optic network was 2,100 km long.7 The government’s goal is to have 110,000 ports for broadband connection across the country by the end of 2015. WiMAX broadband was first introduced on the Uzbek market by the state-owned operator Uztelecom in 2006 and a private operator in 2008.

More people access the internet at work (state institutions and businesses) than in private households. In the wake of the fast-paced implementation of e-governance initiatives, internet coverage was extended to the entire state apparatus, reportedly also reaching all bodies of local governance (hokimiyats) at the regional and city levels in Uzbekistan by the end of 2013.8 In 2013–2014, the state began to install computers in every mahallah committee—traditional local community councils that the government has turned into an official system for public surveillance and control.9 Still, civil servants’ access to the internet and social media channels for personal use is largely restricted by technical tools as a result of information security concerns.10

Public access points such as internet cafes remain popular, particularly among young internet users. However, since December 2010, minors are officially prohibited from visiting internet cafes without parents or adults between 10:00 p.m. and 6:00 a.m.11 Reportedly, since 2011, students are also not allowed to visit internet cafes between 8:30 a.m. and 7:00 p.m.12 Since September 2005, other public access points such as libraries, schools, universities, museums, and youth organizations must connect to the internet exclusively via the national intranet, a local access and information network called ZiyoNET.13 In July 2013, in a new attempt to limit and control internet access, the government allowed the state-owned telecommunications operator Uztelecom to serve as the exclusive provider of access to ZiyoNET across these target institutions nationwide.14 (Previously, any private ISP could exercise that right on a competitive basis).15 Uztelecom provides unlimited traffic connections to the ZiyoNET intranet via xDSL, FTTx, and CDMA-450 technologies (in rural and remote areas) but limits traffic to the internet on a monthly basis. Currently, the highest internet access speed of 1 Mbps is available for a monthly tariff of UZS 1,441,101 (US$650).16

Expensive access prices, slow speeds, and limits on data volume also curb internet use, in addition to...
the centralized telecommunications infrastructure. Internet subscriptions in Uzbekistan conform to a two-tiered system: access to the TAS-IX peering center and content delivery network, and internet access routed via Uztelecom’s network. Uztelecom and private ISPs provide free access to the TAS-IX network at a maximum download speed of 2 Mbps to their customers. None of the ADSL/FTTB subscriptions from private ISPs enable internet download speeds faster than 2 Mbps (subscriptions are available for an average of US$44 per month and with free traffic up to 12 GB). A basic ADSL subscription for a 256 Kbps minimum download speed is currently available for US$14-$24 per month (with free traffic from 2.4 GB to 4.8 GB).  

Uztelecom remains a leader in the provision of FTTB broadband internet to private households and businesses. However, neither Uztelecom nor private ISPs offer limitless capacities for data transmission on their networks. “Traffic without limits” ADSL/FTTB subscriptions advertised by all ISPs in fact entail quotas on traffic. If a quota is exceeded, the connection speed sharply decreases. For example, Uztelecom offers private households “unlimited” FTTB subscriptions for US$135 per month with a 4 Mbps maximum download speed that drops to 128 Kbps after customers exceed the data volume quota of 30 GB.  

According to official statistics, at least eight leading private ISPs have transferred Uztelecom’s price reductions to their individual subscribers and dropped subscription prices between 15 and 80 percent from 2011 to 2013. At the same time, according to the ITU, internet access prices are still prohibitively expensive in comparison to the average household income. Actual speeds experienced by internet users are frequently much lower than advertised. Users experience frequent disconnections and generally complain about poor quality of connections and technical support on behalf of ISPs.

Restrictions on Connectivity

The state-owned national operator Uztelecom is the primary carrier of Uzbekistan’s telecommunications infrastructure and an upstream ISP. Since August 2005, Uztelecom has operated the national-level backbone network and requires private ISPs to route and transmit their international traffic through its International Centre for Packet Switching (“Mezhdunarodnyi tsentr paketnoyi kommutatsii”). Uztelecom also sells internet traffic to private ISPs at a wholesale, U.S. dollar-denominated price. Uztelecom controls the country’s external internet gateway capacity, which allows the authorities to control access speeds for the entire country, if needed. As of May 2015, the average speed of internet access reached 19.25 Mbps, according to Uztelecom, although Akamai reported average speeds of only 2.6 Mbps for 2014. In 2011, the government prohibited private ISPs from bypassing

17 See, e.g., a tariff list from the leading ISP provider: TPS, accessed April 26, 2013 http://www.tps.uz/tariffs/section/jet  
20 As reported by ITU in 2012, internet access prices were prohibitively high in Uzbekistan and exceeded the monthly GNI per capita level at the rate of approximately 188 percent. See ITU, “Measuring the Information Society: 2012.”  
22 Uztelecom, “АК «Узбектелеком» имеет техническую возможность увеличить скорость внешних каналов Интернет более чем в четыре раза” [JSC «Uzbektelecom» has the technical capability to increase the speed of external Internet channels in more than four times], January 8, 2014, http://www.uztelecom.uz/ru/press/news/2014/2127/.  
Uzbekistan

Uztelecom’s infrastructure to connect to the internet, and from installing and maintaining their own satellite stations in order to establish internet connectivity.

The TAS-IX peering center and content delivery network, established in February 2004, interconnects the networks of 37 private ISPs to enable traffic conveyance and exchange at no mutual charge and without the need to establish international internet connections via Uztelecom. TAS-IX ISPs are challenged to find the income streams for the investments needed to meet the capacity requirements of their customers. Private ISPs provide no traffic limitations to websites hosted within the TAS-IX networks, but filter and block content and applications to the same extent as Uztelecom. Most censorship takes place at the country’s international internet connection, operated by Uztelecom, which aggregates the private ISPs’ traffic at a single node within its infrastructure.

ICT Market

Currently, five mobile phone companies operate in Uzbekistan. The fewest number of subscribers belong to two CDMA operators—Uzmobile (a brand of the state-owned Uztelecom) and Perfectum Mobile (owned by the Uzbek company Rubicon Wireless Communication). There are two GSM operators: Beeline (owned by the Russian VimpelCom Ltd) and Ucell (owned by the Swedish-Finnish company TeliaSonera). In December 2014, UMS (Universal Mobile Systems) entered the domestic market. This company is a joint venture of the Uzbek government (which owns 49.99 percent) and the Russian company MTS, under an agreement reached before the International Centre for Settlement of Investment Disputes of the World Bank. Previously, from July 2012 through April 2013, the government took steps to terminate the operations of the former leading GSM operator Uzdunrobita (a wholly owned subsidiary of the Russian MTS), which had a customer base of more than 9.5 million subscribers. In December 2013, local authorities placed assets and equipment expropriated from Uzdunrobita into the custody of Uztelecom for an unspecified duration and without the right of use.

By 2017, competition within the mobile communications market in Uzbekistan may shrink further. On February 12, 2014, President Karimov signed a resolution that gave CDMA provider Uzmobile the legal status of a “national operator of mobile communications.” With the aim of ensuring a “reliable and stable operation of mobile communications networks given the requirements of information security,” the company is entrusted with the nationwide “introduction of the most innovative technologies for high-speed data transmission, including internet broadband, mobile TV services, e-payments and e-commerce” based on GSM technology. From 2014-2017, Uzmobile will enjoy tax exemptions and licensing privileges in order to reach a target of 7,000 base stations and 8 million subscribers.

26 TAX-IS participating ISP maintain a service to find out whether a website is in the TAS-IX network. See, e.g., TPS, “Проверить, находится ли сайт в сети TAS-IX,” [link]
28 “Russia’s MTS will return to Uzbekistan by the end of 2014,” The Times of Central Asia, August 4, 2014, [link]
Uzbekistan

subscribers by the end of 2017. The Chinese government has pledged US$500,000 in investments for Huawei Technologies to be an official supplier of telecommunications equipment to Uzmobile.31

Service providers are required to have a license to operate, and in 2005, the Cabinet of Ministers adopted Resolution No. 155, which stipulates that telecommunications providers must first register as a legal entity before being issued a license. Thereafter, the licensing procedure is fairly straightforward but in practice is often encumbered by political interests, with applicants from outside the government’s inner circle regularly denied licenses for unjustifiable reasons.32 As of March 2014, no licenses can be given to an internet cafe if the business premises are located in the basement of multistory buildings.33

Regulatory Bodies

In February 2015, the Cabinet of Ministers created the Ministry for the Development of Information Technologies and Communications (MININFOCOM) to consolidate state development and control of the ICT industry. The Ministry is responsible for internet content regulation in order to prevent, among other things, the internet’s “negative influence on the public consciousness of citizens, in particular of young people.” To do so, the Ministry implements measures on the further development of the national segment of the internet (the intranet), as well as the provision of the necessary technical and favorable conditions for the development of “modern national websites on different issues, including information resources to satisfy informational and intellectual needs of the population, particularly of the youth.”34

The Computerization and Information Technologies Developing Center (Uzinfocom) under the Ministry administers the “.uz” top-level domain. There are seven private ISPs officially authorized to provide registry services in the “.uz” domain zone.35 Uzinfocom is also the largest provider of web hosting services, including for the e-government project, government-backed intranet, national search engine, and social-networking sites.36 Current rules for the assignment, registration, and use of the country’s top-level domain create an obstacle to internet access.37

Limits on Content

The government of Uzbekistan engages in pervasive and systematic blocking of independent news and any content that is critical of the regime, particularly that which is related to foreign and domestic

32 IREX, “Uzbekistan.”
37 Law RU “On Telecommunications,” at Arts. 8, 11.
Uzbekistan

affairs or the human rights situation in the country. Access to online information was relatively open until 2001, when the authorities began filtering politically sensitive websites and reportedly intercepting email communications. Online censorship and surveillance significantly intensified after May 2005, following the government’s violent crackdown on peaceful antigovernment protests in Andijan and the subsequent news blackout on this event in the traditional media.

Blocking and Filtering

Websites permanently blocked in Uzbekistan do not appear on www.поиск.uz—the national search engine of Uzbekistan’s government. Blocked websites include most independent news websites with socio-political and human rights-related content on Uzbekistan. Websites of Uzbek human rights and opposition groups in exile are also blocked. The websites of the international broadcasters Radio Free Europe/Radio Liberty, Deutsche Welle, and the Uzbek services of the BBC and Voice of America have been permanently inaccessible in Uzbekistan since 2005. Websites of the major international human rights organizations, such as Amnesty International, Freedom House, and Human Rights Watch, among others, are also blocked.

Stringent limits on content also appear on the ZiyoNET information network, which is the only mode of internet access for libraries, educational and other cultural institutions, and youth organizations. In July 2013, the government adopted a resolution calling for the introduction of an official list or registry of information resources to be made available on ZiyoNET after having received approval by the respective state bodies. As of February 2014, there were 50,100 “approved” educational resources, some of which are knock-offs of popular social media platforms, such as Utube.uz, which is similar to YouTube.

Several government-linked entities monitor and control online communications, though the opaque system offers few details on how decisions are made or what websites are blocked at any given time. The Center for the Monitoring of the Mass Communications Sphere takes various measures to maintain compliance with national legislation that restricts free expression. Among its key objectives are “to analyze the content of information disseminated online and ensure its consistency with existing laws and regulations.” Based on its systematic monitoring of online content, the center

Uzbekistan

has contributed to the takedown of independent websites (see Media, Diversity, and Content Manipulation). The Expert Commission on Information and Mass Communications, a secretive body established in August 2011, oversees the Monitoring Center. The commission is not independent and must submit quarterly reports to the Cabinet of Ministers. Furthermore, its membership is not public, although the body is reportedly comprised exclusively of government employees. The new commission is mandated to evaluate online publications and determine if they: have a “destructive and negative informational-psychological influence on the public consciousness of citizens;” fail to “maintain and ensure continuity of national and cultural traditions and heritage;” or aim to “destabilize the public and political situation,” or commit other potential content violations.

The commission also assesses publications referred to it by the Monitoring Center or other state bodies, including the courts and law enforcement, drawing on a designated pool of government-approved experts. The experts submit reports to the commission, whose members then vote on whether or not a violation has been committed. If a violation is found, the decision becomes the basis for action to be taken by state bodies, including courts, and by “other organizations,” presumably private ISPs. There are no procedures in place that require notification of those whose content is affected by the decision or that grant them an opportunity to defend the speech in question, nor is there a clear avenue to appeal the decision after it is made. The broadly defined violations and wide discretion granted to the commission raises concerns of how it could be used to suppress or punish free speech—including ordering ISPs to delete content or encouraging the arbitrary imprisonment of bloggers—particularly given the Uzbek government’s track record of politically motivated censorship.

Content Removal

Intermediaries can be held liable for third-party content hosted on their platforms and can be forced to remove such content. Following the 2007 amendments to the 1997 law “On Mass Media,” any website engaged in the dissemination of mass information periodically (at least once every six months) is considered “mass media” and is subject to official press registration. This procedure is generally known to be content-based and arbitrary, and inhibits editors and readers from exercising

49 Ibid, Annex I, contains a list of the Commission’s members that is not made public.
50 Reporters Without Borders, “Uzbekistan.”
51 Resolution of the Cabinet of Ministers RU, No. 228, at art. 1 and Annex II, art. 5. See note 50 above.
their freedom of expression and right to access information. As of January 2015, 304 news-oriented websites, including online versions of traditional news media outlets, were registered as mass media in Uzbekistan.

In September 2014, amendments to the Law on Informatization were passed stipulating that owners of a blog or other news source published exclusively online, including citizen journalists unaffiliated with traditional news media outlets, fall under state regulation. By the law’s broad definition, any person may qualify as a blogger by engaging in the dissemination of any types of information ("of socio-political, socio-economic and other character") to the public through a website, including for the purpose of its discussion by users. For the purpose of content restrictions, the law seems to equate blogs with traditional news media. In the process of gathering information, owners of a blog or website have to substantiate with evidence the credibility (dostovernost) of "generally accessible information" prior to its publication. This requirement would also apply to individuals reposting information, and would oblige them to "immediately remove" the posted information if it is not credible. In cases of noncompliance, the law entitles a special governmental body to limit access to the website. In cases of news-oriented blogging, bloggers may have difficulty in obtaining protection equivalent to that granted by the state to professional journalists, as these rights are elusive in practice.

Media, Diversity, and Content Manipulation

The online media environment in Uzbekistan is severely restricted. Self-censorship is pervasive, given the government’s tight controls over the media and harsh punishment of those who report on topics deemed “taboo,” including criticism of the president, revelations about corruption, or health education. As a result of the government’s history of harassing traditional journalists, as well as their families, many online writers are cautious about what they post. The editorial direction of the online versions of state-run news outlets is often determined by both official and unofficial guidelines from the government.

Several independent news sites have been shut down as a result of permanent and systematic monitoring of the internet by the Monitoring Center. In May 2015, the court ordered the closure of the news media website Naviyvek, a weekly newspaper established in January 1992 and known for its balanced news reporting. In the past, there have been a few cases of independent news websites officially registered in Uzbekistan being closed or retroactively unregistered in arbitrary fashion (for example, Informator). As of May 2015, Olam remained closed after going offline for “technical reasons” on January 19, 2013. By then, Olam was Uzbekistan’s second most-visited news site. Reportedly, the Uzbek authorities had opened up proceedings against its editor-in-chief and the website owner, the Tashkent-based LLC Mobile Mass Media. Charges included infringement of copyright.
Uzbekistan

and patent law, high treason, encroachment upon the constitutional order, espionage, subversive acts, loss of documents containing state or military secrets, and robbery. Prior to its closure, Olam had reported on state appropriation of an Uzbek subsidiary of the Russian MTS mobile company in 2013-2014.

Under the 1999 Law on Telecommunications and several other government resolutions, the licenses of lower-tier ISPs may be withheld or denied if the company fails to take measures to prevent their computer networks from being used for exchanging information deemed to violate national laws, including ones that restrict political speech. Under Order No. 216 passed in 2004, ISPs and operators “cannot disseminate information that, inter alia, calls for the violent overthrow of the constitutional order of Uzbekistan, instigates war and violence, contains pornography, or degrades and defames human dignity.” Given these broad restrictions, many individuals and organizations prefer to host their websites outside the country.

The government has also placed political pressure on mobile phone operators. In March 2011, amid growing unrest in the Middle East, regulators demanded that operators notify the government of any attempts to circulate mass text messages with “suspicious content” and reportedly warned that the providers would be required to shut down internet connections provided to mobile users at the authorities’ request.

Facebook, YouTube, Twitter, and the Russian social networks Odnoklassniki and VKontakte continue to top the list of the most visited websites in Uzbekistan. In 2014, Facebook was the fourth most visited website in the country, followed by Odnoklassniki (available in Uzbek since December 2012), VKontakte, and YouTube. Twitter became particularly popular in the fall of 2013, when the president’s daughter Gulnara Karimova used her account to reveal inside secrets about her family and the corrupt practices of the Uzbek national security service.

As social-networking sites and blogging platforms have grown in popularity, the government attempts to influence the information circulated on them by creating and promoting Uzbek alternatives to popular global or regional brands. The most recent example is the microblog Bamboo, launched in February 2014 for exclusive use by the Uzbek people under the motto “one country, one network.” The platform is very similar to Twitter and is likely to have been developed by the state to reduce the use of Twitter in Uzbekistan. According to Bamboo’s terms of use, any information about its users can be forwarded to official bodies upon their “lawful and legitimate requests.” Also in February 2014, local IT specialists developed a messaging platform called Gap IM as an alternative to messaging services available via Skype, ICQ, Google Talk and Mail.ru. The service is available in Russian and Uzbek languages and can be used on mobile phones.

Uzbekistan

The role of blogs as opinion-shaping media on political and social issues in Uzbekistan is minimal. The blogosphere is largely of entertainment character. A handful of blogs critical of the regime are run by Uzbek dissidents (for example, Jahonnoma, Turonzamin, and Fromuz) or are affiliated with independent online news websites and run by invited journalists. Since its establishment in January 2012, the Choyxona forum has become somewhat popular, with over 1,500 threads, 58,000 posts, and 736 members as of February 2014. It is run by the former editors of Arbuz, a forum site that was suspended in 2011 after Uzbek authorities arrested several of its users.

Digital Activism

A handful of political activists and regime critics actively use the internet and social media as channels to reach supporters in and outside of Uzbekistan. Their efforts may have the effect of raising awareness about the issues at stake, but their actual impact on social mobilization is limited, largely due to the repressive environment for freedom of speech and the right of assembly within the country. Moreover, the stringent ideological policies of the government regarding the use of the internet and social media by Uzbek youth seem to discourage digital activism as a form of political engagement among young people in particular.

In February 2015, the banned opposition group Birdamlik and human rights defender Mutabar Tadjibaeva protested against the unconstitutional presidential elections of March 29, 2015, by staging their own virtual alternative election. The organizers launched a virtual election committee’s website at Saylov2015.org, where people could cast a vote for eleven presidential candidates (excluding President Karimov). The major goal was to engage the public in Uzbekistan in the virtual exercise of free and fair elections and promote democracy. Unsurprisingly, prior to the official election date, hackers defaced the website with pornographic images and the website is no longer available.

Violations of User Rights

The extent of state interference with internet users’ rights, such as freedom of speech and the right to privacy, is a cause of serious concern. State measures to silence dissent include persecution and criminal prosecution of regime critics and independent journalists, often on fabricated charges, as well as systematic and permanent media censorship and constant surveillance of communications. A freelance reporter for an independent online media outlet was prosecuted and fined by a court in June 2014 for working without the appropriate license after he published an article about the government ordering the demolition of buildings in Tashkent and failing to compensate residents. The 10-year-old independent news website Uznews ceased operations after confidential information leaked by hackers exposed its reporters in Uzbekistan to possible retaliation from the government. As of May 2015, one Uzbek internet user was serving an eight-year prison sentence for violating constitutional order by establishing communication over the internet with an Uzbek opposition group in exile and for distributing materials on the group’s orders.

---

Uzbekistan

Legal Environment

Uzbekistan’s constitution protects the rights to freedom of expression and of the mass media, as well containing bans on censorship. However, the implementation of these protections is minimal under the current authoritarian regime with its weak attachment to democratic principles. National courts have generally failed to protect individuals, including professional journalists, against government retaliation for exercising their free speech rights. Rampant corruption, particularly within law enforcement bodies, as well as weak legislative and judicial bodies, continue to have a deleterious impact on freedom of speech.

Article 29 of Uzbekistan’s constitution guarantees the right to gather and disseminate information. The Uzbek criminal code contains several provisions that have been used extensively to prosecute reporters and internet users for online activities. They include but are not limited to the crimes of threatening constitutional order (Article 159), production and dissemination of materials containing a threat to public security and order with foreign financial help (Article 244), slander (Article 139), insult (Article 140), and insult of the president (Article 158). Both slander and insult are punishable with fines ranging from 50 to 100 times the minimum monthly wage, correctional labor of two to three years, arrest of up to six months, or detention for up to six years. Further restrictions typically placed on journalists and internet users are based on vague information security rules.

Prosecutions and Detentions for Online Activities

The regime’s hostility towards its critics, including independent journalists, human rights activists, and critically-minded internet users, is notorious in Uzbekistan. As of May 2015, two Uzbek online journalists remained in jail on criminal charges presumed to be fabricated. Solidzhon Abdurakhmanov, a 63-year-old journalist and former reporter for Uznews (the independent news website forced to shut down in December 2014) continues to serve a 10-year sentence imposed in October 2008 for allegedly selling drugs. Prior to his arrest, he had reported on human rights and economic and social issues, including corruption in the Nukus traffic police office, which fueled suspicions that the drug charges were trumped up in retaliation for his reporting. Dilmurod Saied, a freelance journalist and human rights activist, is serving a 12.5 year sentence imposed in July 2009 on extortion charges. Before his detention, he had reported on government corruption in Uzbekistan’s agricultural sector for local media and independent news websites.

In a summary administrative trial on June 28, 2014, well-known freelance journalist Said Abdurakhimov (pseudonym “Sid Yanyshev”) was found guilty of two administrative offenses and fined US$4,100 for an article about the government’s failure to compensate local residents in Tashkent for demolishing their houses. The article was published on Fergananews, a website blocked in Uzbekistan. Abdurakhimov was convicted under Articles 165 and 184 of the code of administrative offenses.

---

es for working as a journalist “without a license or permit” and “preparing or keeping information representing a threat to public security and order, with the aim of disseminating it.” Following the court’s reasoning, any persons who engage into the process of newsgathering are functionally indistinguishable from traditional journalists operating without a license required by law; however, this court case took place before the legislation was amended in September 2014 to extend media liability to bloggers and other website owners disseminating information to the public.

Since January 2012, the fate and whereabouts of Jamshid Karimov remain unknown. An independent journalist and human rights activist who also happened to be the president’s nephew, Jamshid Karimov was known for his critical reporting under different pseudonyms for independent news websites, including Fergananews, Uznews, and the Institute for War and Peace Reporting. In September 2006, he was abducted in Djizak during a hospital visit to his mother, detained incommunicado for 13 days, and was then confined to a Samarkand psychiatric hospital. Until his release in November 2011, he was under forced psychiatric treatment for “sluggish schizophrenia,” a diagnosis invented and systematically used in the USSR to silence political dissent.

Given these events, which are believed to have been in retaliation for his professional activity, there is a strong suspicion that Jamshid Karimov has been subject to involuntary disappearance for more than three years, which constitutes torture and cruel and inhuman treatment under article 7 of the International Covenant on Civil and Political Rights, which has been ratified by Uzbekistan.

Cases of selective and arbitrary prosecution of both independent and licensed journalists for their online publications have taken place in the past. They include Abdumalik Boboyev, a reporter for Voice of America’s Uzbek Service, Vladimir Berezovsky, the editor of Vesti, Viktor Krymzalov, a reporter for Centrasia and Fergananews, and Elena Bondar, a reporter for Uznews and Fergananews. Some of these journalists were convicted under criminal law and had to pay exorbitant fines as a punishment. These cases have shown that recommendations by the internet state censorship authority, the Monitoring Center, which determines which online news articles violate national legislation, are being used to legitimate prosecution and conviction of online reporters.

Surveillance, Privacy, and Anonymity

The space for anonymous online communication in Uzbekistan is steadily shrinking, and government surveillance of ICTs is extensive. Although Article 27 of the constitution guarantees the privacy of “written communications and telephone conversations,” there is no data protection legislation in Uzbekistan. Since 2006, the National Security Service (NSS) conducts electronic surveillance of the national telecommunications network by employing the “system for operational investigative measures” (SORM), including for the purposes of preventing terrorism and extremism. ISPs and mobile phone companies must install SORM and other surveillance equipment on their networks in order

---

Uzbekistan

to obtain a license.\textsuperscript{82} Telecommunications providers are prohibited by law from disclosing details on surveillance methods and face possible financial sanctions or license revocation if they fail to design their networks to accommodate electronic interception.\textsuperscript{83}

The NSS systematically eavesdrops on citizens’ communications over email, mobile phone and Skype, in online forums, and social networks. There is no independent oversight to guard against abusive surveillance, leaving the NSS wide discretion in its activities.\textsuperscript{84} If surveillance is part of a civil or criminal investigation, content intercepted on telecommunications networks is admissible as court evidence.\textsuperscript{85}

There are no explicit limitations on encryption, though in practice the government strictly regulates the use of such technologies.\textsuperscript{86} Proxy servers and anonymizers remain important tools to access content blocked in Uzbekistan. However, in September 2012, Uztelecom started a centralized and permanent blocking of proxy servers and websites listing free proxies without a web interface. At the same time, the use of both proxies and anonymizers require computer skills beyond the capacity of many ordinary users in Uzbekistan.

In 2011, Arbuz, one of the country’s most important online forums for anonymous discussion, was shut down after the arrests of several users. The site’s founder told media that several people who had been active contributors to a forum about Kyrgyz-Uzbek ethnic clashes in 2010 had been detained. According to some reports, the NSS had tracked them through their internet protocol (IP) addresses.\textsuperscript{87} Few options remain for posting anonymous comments on other online forums—such as Uforum,\textsuperscript{88} which is administered by the state-run Uzinfocom Center—as individuals are increasingly encouraged to register with their real names to participate in such discussions.\textsuperscript{89} Individuals must also provide a passport to buy a SIM card.\textsuperscript{90}

Since July 2004, operators of internet cafes and other public internet access points are required to monitor their users and cooperate with state bodies. Following regulatory amendments in March 2014, the situation concerning respect for privacy and the protection of personal data of internet cafe users has deteriorated further.\textsuperscript{91} Operators of internet cafes and public access points must

\textsuperscript{82} Ibid, art. 5.8. Infra., note 110. Also, tax and custom exemptions apply for import of the SORM equipment by domestic ISPs, see Tax Code of RU, art. 208, 211, 230 part 2, and 269.

\textsuperscript{83} See Law RU, “On Telecommunications”.


\textsuperscript{90} MTC Uzbekistan, “How to subscribe,” http://www.mts.uz/ru/join/

\textsuperscript{91} See Resolution of the SCCITT RU, “О внесении изменений и дополнений в Положение о порядке предоставления доступа к сети Интернет в общественных пунктах пользования [On making amendments and additions to the Regulations on the procedure for providing access to the Internet in the public areas of use],” March 19, 2014, No. 79-xx, SZRU (2014) NO. 13, item 150.
install surveillance cameras on their premises as a new measure to “ensure [the] safety of visitors.” Additionally, they are required to maintain a “registry of internet web-resources (logfiles)” used by customers and to retain this information for a period of three months. In practice, compliance with these measures can become burdensome and expensive for internet cafe businesses in Uzbekistan.

Intimidation and Violence

While there have been no reports of government agents physically attacking bloggers or online activists, the National Security Service (NSS) has been known to employ various intimidation tactics to restrict freedom of expression online. For example, in June 2011, there were reports of NSS officers confiscating electronic media devices at the airport, checking browsing histories on travelers’ laptops, and interrogating individuals with a record of visiting websites critical of the government.92 Further, on February 12, 2014, Marjam Ibragymova, a political scientist from Tashkent, was invited by prosecutors for a “prophylactic talk,” during which they threatened her with criminal charges of libel and the dissemination of materials threatening to public security and order. The materials included online articles she wrote for Uznews and Fergananews under the pseudonym “Gulsara Vafaeva,” as well as views she expressed during an Uznews talk-show online. She was compelled to sign a statement on the “inadmissibility of such actions in the future.”93

Technical Attacks

In November 2014, hackers took over an email account linked to Uznews, a leading independent news media website that has been permanently blocked in Uzbekistan since 2006. Confidential financial information from the email account of the website’s editor, Galima Bukharbayeva, was then leaked onto the internet. The confidential data also contained the names of Uzbek citizens engaged in newsgathering for Uznews. On December 19, 2014, the editors decided to close the site on the grounds of concern over the safety of its reporters in Uzbekistan whose identities were leaked.94 Galima Bukharbayeva received the Committee to Protect Journalists’ International Press Freedom Prize in 2005 for her Andijan coverage. Uznews had been engaged in critical reporting on Uzbekistan over the last 10 years.

Distributed denial-of-service (DDoS) attacks on independent news media websites reporting on Uzbekistan, including the websites Centrasia.ru, Fegananews.com, Uznews.net, UzMentronom.com, and Ozodlik.org (Uzbek service of Radio Free Europe/Radio Liberty), have been frequent in the past and continue to take place.

In September 2013, a government resolution established the Information Security Centre as the new centralized arm of the State Committee on the CITT dealing with the security of “the national segment of the internet” and state information networks, including the e-governance infrastructure.95

95 Resolution of the Cabinet of Ministers of RU «О мерах по организации деятельности Центра развития системы Электронное правительство и Центра обеспечения информационной безопасности при Государственном комитете связи, информатизации и коммуникационных технологий Республики Узбекистан» [On Measures Establishing the Development Centre on «E-governance» System and Cybersecurity Centre at the State Committee on the CITT], No. ПП-2058, September 16, 2013, SZRU (2013) No. 38, item 492, art. 3.
Uzbekistan

The Centre took over the functions and competences of the Uzbekistan Computer Emergency Readiness Team (UZ-CERT), established in 2005. In particular, the Centre continues to alert internet users to security threats and give recommendations on the protection of digital information. The Centre interacts with domestic ISPs, mobile phone operators, and state bodies—including law enforcement—on the prevention and investigation of “unsanctioned or destructive actions in information space.”

96 See Resolution of the President RU No. ПП-2058, note 39 above (check cross-reference), at Annex 3, art. 1
Venezuela

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>21</td>
<td>22</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>56</td>
<td>57</td>
</tr>
</tbody>
</table>

Population: 30.2 million
Internet Penetration 2014: 57 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2015 Status: Not Free

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- In the wake of protests against the government, arbitrary arrests of social network users increased. At least eight Twitter users were arrested between August and October 2014, and most of these users remained detained without due process as of May 2015 (See Prosecutions and Detentions for Online Activities).

- In November 2014, only one month after numerous social media users were arbitrarily arrested, the ruling party proposed an amendment to the country’s cyberterrorism law that would make it a crime to use social networks to “disrupt public peace” (See Legal Environment).

- Over 1,000 websites were blocked between November 2013 and October 2014. Although most were sites that listed the black-market dollar exchange range, at least two prominent news websites were also blocked during the coverage period (See Blocking and Filtering).

- Venezuela, which has the slowest internet in the region after Cuba, was one of only two countries globally that saw a decline in average internet speeds in 2014. Frequent electricity outages and unexplained, prolonged interruptions of internet service presented further obstacles to access. (See Availability and Ease of Access and Restrictions on Connectivity).
Introduction

In the midst of a worsening economic crisis, declining popularity for President Nicolás Maduro, and upcoming parliamentary elections, the government has increased efforts to maintain control of the media. The National Telecommunications Commission (CONATEL) ordered arbitrary blocking of websites without due process, while the dominance of the government-owned internet service provider, CANTV, facilitated these blockings.

During the coverage period, at least eight online users were detained under sweeping laws that prohibit any content that threatens public order or promotes anxiety in the public. In the wake of active protests on social media, the government has announced the possible enactment of new laws to limit digital activism and access to information online.

Less overt limitations on online freedom stem from financial restrictions that limit investments in telecommunications infrastructure. Poor access and low quality connections continue to plague the country. Although official government data shows that internet penetration was over 60 percent by the end of 2014, connection speeds are still very low, with an average connection speed of around 1.4 Mbps.

Even as the government tightens its grip on the media by neutralizing media outlets, launching pro-government outlets, and restricting access to foreign currency needed to import newsprint, citizens have continued to create vibrant communities and discussions through digital media and social networks. The past year marked the creation of new digital ventures, which will add diverse voices to the digital landscape. Meanwhile, a number of new cell phone applications and Twitter feeds have adapted to help Venezuelans, some of the region’s most active social media users, battle continuous shortages in the midst of the economic crisis.

2 In June 2015, officials announced that the legislative election is scheduled for December 2015.
6 Dylan Baddour, “Periodistas en Venezuela se mudan a la red por aumento de presión del gobierno,” [Journalists in Venezuela Move to the Net Due To Increased Government Pressure] Blog Periodismo en Las Americas, The Knight Center at the University of Texas Austin, October 13, 2014, http://goo.gl/6yA3qY.
Venezuela

Obstacles to Access

Internet penetration in Venezuela remains extremely uneven, with a significant divide between rural and urban areas. The quality of internet access is also low, a problem exacerbated by the restricted access to foreign currency, which has led to deterioration of telecommunication infrastructure. Blackouts of electricity are common, especially in smaller, rural cities where they frequently last many hours and sometimes even days. Although a number of private internet service providers (ISPs) operate, the state-owned provider claims a majority of the backbone infrastructure and accounts for around 65 percent of all internet subscriptions. Some experts have raised the possibility that service failures on the part of the state-owned provider were purposeful, as they often coincided with moments of increased political tension.

Availability and Ease of Access

Although internet penetration continued to increase in Venezuela, the quality of the connection is low. Excessively slow speeds, frequent service failures, and unreliable electricity leave many people with limited or no internet access.9 The problem is exacerbated in rural areas where internet penetration is much lower compared to the capital, despite some government initiatives to expand access. A complicated system of currency controls renders foreign currency inaccessible and hampers private investments in telecommunications infrastructure. 10

The International Telecommunication Union estimates that internet penetration increased from 33 percent in 2009 to 57 percent at the end of 2014,11 which puts Venezuela’s penetration rate at the average for the region.12 Venezuela’s National Telecommunications Commission (CONATEL) provided a similar estimate, measuring internet penetration at 60 percent in 2014, with 3.7 million subscribers and close to 16 million users.13 Notably, last year CONATEL only measured internet penetration at 43 percent.14 Although this appears to represent a 14 percent increase over the course of one year, the increase is actually the result of modification of CONATEL’s methodology, which now counts internet users seven years and older who have at least a data plan on their cellphones.15

The vast majority of internet subscribers in Venezuela have broadband internet, although speeds typically fall below the normal broadband threshold. Out of 3.7 million internet subscriptions measured by CONATEL, 94 percent are broadband and seven percent are dial up connections.16 Of these


The government has made an effort to increase connections, launching the Wi-Fi Plan for All in 2013 in order to introduce Wi-Fi in public spaces. Although this plan has introduced Wi-Fi in some areas, it has not met demand.\footnote{Herberto Alvarado, “Internet en Venezuela atraviesa peligroso atraso,” Últimas Noticias, March 23, 2014, http://bit.ly/1NXacmb.} Meanwhile, the National Transportation Network, an ambitious plan by CANTV to set up about 20,000 kilometers of fiber-optic cable is progressing very slowly.\footnote{María Emilia Jorge, “Redes públicas de Wi-Fi no alcanzan para todos,” Public Wi-Fi Networks are not enough for everyone] El Nacional, September 7, 2014, http://goo.gl/aEXgAI.} The government claims that the Simón Bolivar satellite has provided internet and mobile connectivity in even the remote reaches of the country, but independent sources could not yet verify these claims.\footnote{Naylett Leonett García and Ibis León Malavé, “Sin fibra óptica no hay Internet que “vuela”, [Without Optic Fiber Internet Does Not “Fly”] Últimas Noticias June 8, 2014, http://goo.gl/0IauhK.}

The quality of internet connections for the majority of the population remains low and has been exacerbated by deterioration in telecommunications infrastructure due to limits imposed on foreign currency.\footnote{Daniel Pardo, “¿Por qué internet en Venezuela es tan lento?” Inside Telecom Vol. XVI# 08. Caracas, Febrero 27, 2015.} According to CONATEL, investment and earnings among private network providers have gone up when measured in the national currency VEF. When measured in terms of U.S. dollars, however, investment and earnings have declined by 64 percent and 54 percent respectively over the last 13 years, with a noticeable impact on operations.\footnote{Jorge Espinoza. En Bs. inversión e ingresos crecieron mds de 2,300% en 13 años: En $, cayeron 64% y 54%. (In Bs, Investment and Revenue Grew More Than 2,300% in 13 years: In $, fell 64% and 54 %.) Inside Telecom Vol. XVI# 08. Caracas, Febrero 27, 2015.} The state-owned provider CANTV has not fared much better in terms of improving quality of service and access speeds.\footnote{“Internet de Venezuela es el más lento de Sudamérica,” Últimas Noticias, August 25, 2014, http://bit.ly/1AUSHRE.} Poor national infrastruc-
Quality of access appears to be deteriorating. According to the Akamai State of the Internet Report, Venezuela, which has some of the slowest internet in the region was one of only two countries that saw a decline in average connection speeds between 2013 and 2014.\(^{29}\) The average internet connection on fixed broadband is around 1.4 Mbps.\(^{30}\) Faster internet connections are concentrated in the capital city and in wealthy areas. For example, a new WiMax provider and a small company that offer speeds up to 25 Mbps market their services in wealthy regions of the country’s capital.\(^{31}\) Among this small minority are elite with access to superior connections; some small initiatives of IPTV have also opened and gained users.\(^{32}\)

With average speeds over 4 Mbps, mobile connection speeds tend to be much faster than fixed-internet connections in Venezuela,\(^{33}\) and the country is increasingly seeing people turn to mobile connections to access the internet. According to CONATEL, the country has 32 million phone lines (a 106 percent mobile penetration rate), and more than 11 million of these cell phone subscriptions had at least a basic data plan in 2014.\(^{34}\) Mobile connections are especially popular among men under 25 who use their phones to access social media.\(^{35}\) Of the 32 million cell phones in the country, 71.9 percent are GSM, 27.5 percent are CDMA (offered by the state mobile provider, Movilnet), and 0.6 percent are LTE.\(^{36}\)

Despite the faster speeds and popularity of mobile phones, the potential for mobile connections is severely constrained by scarcity and high prices of smartphones in the country. The 11 million phones with data plans represent only about 35 percent of the total number of cell phones in the country, and smartphones are increasingly expensive and scarce.\(^{37}\) Limits on foreign exchange have made it difficult for mobile companies to import phones, resulting in a significant shortage of cell phones and rampant speculation.\(^{38}\)

In December 2014, the government granted concessions for the operation of 4G LTE networks to three telecomm operators (the state owned Movilnet, Movistar, and DirecTV);\(^{39}\) prior to these concessions only one company (Digitel) offered 4G to around 200,000 subscribers.\(^{40}\) As of May 2015, however, 4G options were still limited to Digitel and Movistar and only available in a few cities. Most

---

28 Associated Press, "Widespread Blackouts Hit Venezuela."
31 The WiMax provider Vivo Play is a company created very recently that has about 40,000 subscribers; See also the internet provider IpNet, [http://goo.gl/GKANW2](http://goo.gl/GKANW2).
33 Akamai, State of the Internet Report, 48.
36 “Venezuela registra más de 30 millones de suscriptores de telefonía móvil.”
38 Espinoza, “The Whys and Wherefores of the $20,000 iPhone.”
Venezuela

mobile subscribers still opt for a low bandwidth option (1 to 1.5 Mbps) because, at 3.5 percent of the minimum wage, these plans are almost half the price of mobile 4G plans, which cost approximately 6 percent of the average monthly minimum wage.

Restrictions on Connectivity

Although exact figures are not available, the state owns the majority of the national level backbone infrastructure through the state provider CANTV. In recent years, the possibility of establishing an internet exchange point (IXP) was discussed, but the government has not indicated whether it will move ahead with this plan in the future. Frequent service failures on the part of CANTV during politically sensitive times have raised suspicions that the government has purposefully restricted internet access to prevent social mobilization on certain occasions.

During the first third of 2015, internet service failures increased in frequency. From January 16-17, 2015, the largest internet provider (ABA, from the state-owned CANTV) had failures at a national level that, in some regions, lasted up to 36 hours. CANTV apologized to the users via Twitter, but questions about the cause of the service interruption were never clarified. Experts have pointed out that although this interruption of service could be a result of the lack of maintenance and investment in the state’s telecommunication platform, it coincided with President Maduro’s return to the country after a trip abroad; an event that some authorities worried might trigger an escalation of street protests. During the same month, CANTV suffered two service failures in the Andean region, which the provider attributed to scheduled maintenance and cuts in the fiber-optic cable. Again, these service failures occurred in a region with high levels of protests.

Although it was not possible to confirm that service failures during the coverage period were the result of purposeful government action, disruption of services during protests or politically important times is a continuing concern in Venezuela. In early 2014, CANTV experienced a 36-hour service interruption in the city San Cristóbal that coincided with an announcement by the administration that the government would take steps to control protests, which had been raging for two weeks by the time service was blocked.

---

43 Personal interviews with a variety of telecommunications experts and information about the holdings of the state-owned Cantv seem to indicate that the government may control roughly 60 percent of the national-level backbone infrastructure.
Venezuela

ICT Market

Although there are a number of private providers, the state dominates the ICT market. Almost 69 percent of users access the internet through the state-owned provider CANTV’s ABA or through the state-owned mobile provider, Movilnet.⁴⁹ The strict foreign currency exchange control, in place since 2003, prevents private companies from repatriating their earnings and accessing the foreign currency necessary for their investments, which has led to the deterioration of their services.⁵⁰ It also creates a substantial barrier to new firms who might seek to enter the market.

CANTV, the only provider to offer ADSL, dominates the fixed broadband market, providing service to more than 67 percent of users in this market.⁵¹ The rest of the population accesses the internet through one of several private telecommunication providers. Seven companies provide cable (pay television) service to 4.5 million subscribers, and three of them also offer internet access via cable modem. The second most widely used ISP, Intercable offers services in major cities. Although it used to offer a connection speed of 10 Mbps, this plan is no longer available; currently, this company is primarily selling its 1MB plan, which is more expensive than the plan offered by ABA.⁵²

The state telecommunication provider is also dominant in the mobile market, with Movilnet, a subsidiary of CANTV, leading the sector with over 16 million users and close to 51 percent of the market share. There are two private mobile providers: Movistar, a subsidiary of the Spanish firm Telefónica with approximately 11 million customers and Digitel, a domestic company, which comes in third with 5 million customers.⁵³

Regulatory Bodies

In addition to owning and operating Venezuela’s leading telecommunications operator, the state also controls CONATEL, the body responsible for regulating and licensing of the telecommunications sector. The Law on Social Responsibility on Radio, Television, and Digital Media (Resorte-ME Law) grants the regulatory body the power to rule over the blocking or deletion of content and to sanction service providers, an ability it has exercised without granting due process to the affected parties (see Blocking and Filtering).⁵⁴

While Article 35 of the Organic Law of Telecommunications provides for CONATEL’s operational and administrative autonomy, the president has the power to appoint and remove the agency’s director and the other four members of its board.⁵⁵ A series of presidential decrees over the past decade has shifted oversight of the commission to various ministries, the vice presidency, and finally, in December 2013, to the Ministry of Communication and Information.⁵⁶ In addition to making oversight near-
Venezuela

ly impossible, these arbitrary shifts in control are evidence of CONATEL's lack of independence from the executive.

Limits on Content

The blocking of webpages in Venezuela follows three main patterns: those ordered directly by CONATEL, those executed by CANTV, and those that are apparently implemented by private ISPs for fear of sanctions from the regulatory body. Although the government has blocked over 1,000 sites since November 2013, the blocking of the Argentine site Infobae and the main domains of the website of the television channel NTN24 drew particular public outcry and international condemnation. Third-party liability encourages self-censorship and content removal, as does the threat of harassment of critical journalists by government sympathizers. Despite these limitations, the online landscape remains vibrant in Venezuela, with increasingly more people using the internet.

Blocking and Filtering

The government regulatory body CONATEL blocked over 1,000 webpages between November 2013 and October 2014 by way of sending a blacklist of sites to CANTV and private ISPs. A report by the journalist William Peña also suggests that the state provider CANTV may have independently decided to block certain sites without necessarily receiving instruction to do so from CONATEL.

Pages publishing the black market dollar exchange rates constituted the vast majority of the blocked sites. Over the past decade the government has instituted a complex series of currency and price controls, granting the state control of almost all foreign exchange. As the crisis engulfing Venezuela’s economy has deepened in the past few years, dollars have become scarce and people have flocked to the black market in droves to access foreign currency. The government has waged a war on the site Dólar Today (Dollar Today), a prominent site run out of Florida which publishes the black market exchange rate, blocking hundreds of URLs in its effort to purge links and re-blogged content from the site.

In March 2015, CONATEL tried to block the mobile app of the Dollar Today platform, and in the process, ended up blocking all of Amazon’s cloud (S3 service) where the app was hosted. This resulted

60 Peña, “Conatel guillotinó la Web.”  
61 Peña, “Conatel guillotinó la Web.”  
63 Manuel Rueda, “Meet the Venezuelan rebel whose crime is publishing exchange rates,” Fusion, June 23, 2015, http://fus.in/1O4ZMm5.
Venezuela

in the collateral blocking of many other applications.\textsuperscript{64} The government has also proposed legislation to further expand its powers to block economic information and transactions. In late-2014, the ruling party proposed legislation that would require all e-commerce transactions in Venezuela to be in Bolivares, Venezuela's national currency, and would grant the government expanded powers to block online commerce.\textsuperscript{65}

Government censorship also extended to news sites with political content.\textsuperscript{66} In September 2014, CONATEL blocked all the domains—including websites, mobile application, and the Facebook page—of the television channel NTN24 in the wake of their critical coverage of a public health crisis in the country. The channel did not receive any notification or explanation from the government.\textsuperscript{67} In October, William Castillo, the president of CONATEL, tweeted\textsuperscript{68} that—following the orders of the minister of communication and information—he ordered the blocking of the news site Infobae for publishing images of the corpse of a murdered representative from the ruling party.\textsuperscript{69} Although NTN24 was unblocked in October 2014, Infobae remains inaccessible within the country.\textsuperscript{70}

In addition to directly ordering blocks, CONATEL successfully exerted pressure in the form of informal emails and calls on private ISPs, who then blocked content in order to avoid potential sanctions.\textsuperscript{71} Almost none of these blockings followed judicial or administrative procedures set out by law, and public entities have repeatedly denied information requests under the argument that information about telecommunications is a state secret.\textsuperscript{72}

Even though there were complaints about the alleged blocking of social media applications, these were not confirmed, with the exception of the blocking of Pbs.twimg.com (the site that hosts images on Twitter) in February 2014, amid widespread protests against the government.\textsuperscript{73} The web application Pastebin was also blocked during the protests and remained blocked as of May 2015.

Content Removal

The Law on Social Responsibility on Radio, Television, and Electronic Media (the Resorte-ME law) establishes liability for third parties for content published on their site and grants CONATEL the discretionary capacity to impose severe penalties for violations.\textsuperscript{74} This legal framework has resulted in

\begin{thebibliography}{9}
\bibitem{67} Espacio Público, "Bloquean dominios de NTN24."
\bibitem{68} William Castillo B, Twitter Post.
\bibitem{69} "Gobierno venezolano ordenó bloquear la página argentina Infobae.com," [Venezuelan government ordered to block Infobae.com] El Universal, October 10, 2014, \url{http://goo.gl/yFm6h}.
\bibitem{71} Internet Society Venezuela, "Libro blanco sobre libertad en Internet," [The white paper on Internet freedom] June 2014, \url{http://bit.ly/1O4ZL1m}.
\bibitem{72} Espacio Público, "TSJ: Toda información sobre telecomunicaciones es secreto de Estado," [TSJ: All information on telecommunications is a state secret] December 4, 2014, \url{http://goo.gl/KfwwU}.
\bibitem{74} The text of the law is available here: Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, 2012, \url{http://bit.ly/1LK14B4}.
\end{thebibliography}
self-censorship and preemptive censoring of content, as webmasters and editors may avoid publishing information that contradicts the government.

Although there are no clear cases in which judicial or extralegal measures were used to force digital media to delete content, observers have commented on the disappearance of politically sensitive information from the digital version of the news site El Universal after the site changed owners in July 2014. At least one YouTube user denounced receiving a takedown request, triggered by a privacy complaint, for a video of the president’s son dancing under a shower of dollar bills at a luxurious hotel. The user appealed, and the video in question is now available on YouTube.

Media, Diversity, and Content Manipulation

The Venezuelan government dominates the digital media landscape. Facing the rise of new digital media, the government has amplified its own voice by launching state-controlled media enterprises, neutralizing alternative media through censorship, and encouraging progovernment social media users to harass the opposition. Meanwhile, censorship and self-censorship have constrained voices critical of the government. The detention of more than eight social media users, some for relatively innocuous posts, may have contributed to fear among online users (see Prosecutions and Detentions).

Many independent media outlets also suffer from serious financial difficulties, which are exacerbated by a shortage of foreign currency and a dependence on revenue from official and private advertising, which may be vulnerable to government pressure. Some cyber activists have expressed suspicion that the capital behind some new digital ventures might come secretly from the government or entities allied with the government. Other observers have noted that the previously very critical media

---

84 Luis Carlos Diaz, Twitter, post, “Nadie sabe RT @luisoliveros13 Aparecen medios electrónicos por montones ¿quienes son los dueños? ¿quienes tienen tanto capital disponible?” [Nobody knows RT @luisoliveros13 new digital media appear in bunches. Who are the owners? How much capital do they have available?] November 6, 2014, http://goo.gl/9tvSAS.
Venezuela

outlet, *El Universal*, seems to have taken a softer tone towards the government under its new ownership by an obscure Spanish investment firm. 85

Although recent instances of online censorship and prosecution for online content show that the government is increasingly turning its attention to online content, in 2014 and 2015 the online sphere remained a vibrant space for political and social expression. Constraints imposed on offline media through buy-outs, restrictions on newsprint and foreign currency, and legal threats have pushed many journalists into the digital sphere, where they have launched approximately a dozen new digital ventures in recent years. 86 Even in cases where editorial censorship or self-censorship has restricted content, some journalists note that they have somewhat more freedom on the web. 87

As political discussions move to the web, the government has sought to expand its digital presence. Some social media specialists have detected and denounced the use of bots and fake accounts to disseminate pro-government tweets. 88 It seems that this mechanism may have been used to further promote the hashtag #ObamaDerogaElDecretoYa (Obama Repeal the Executive Order), which demands that the president of the United States nullify the executive order that suspends visas and freezes assets of government officials whom the U.S. government deems to be linked to cases of corruption and human rights violations. 89 Researchers have also found evidence that government critics may use automatic platforms to disseminate tweets. 90

Many users have criticized the digital sphere for its incredible polarization between opposition and government voices, leaving little room for independent commentary. 91 Issues that are not actively politicized by one side or the other are often ignored entirely. Government supporters and critics have engaged in a hashtag war, with each side competing for attention in the digital sphere. 92

Digital Activism

With over 12 million Facebook users and 4 million Twitter users, Venezuelans are very active on social media. 93 Both pro-government supporters and opposition leaders have organized large social

---

86 Dylan Baddour, “Journalists move online in Venezuela as government pressure on media companies grows,” *Journalism in the Americas Blog*, The Knight Center at the University of Texas Austin, October 13, 2014, http://bit.ly/1nNA4j; See also John Otis, “In Venezuela, online news helps journalists get their voices back,” Committee to Protect Journalists (blog), June 1, 2015, https://cpj.org/x/6124.
87 Otis, “Venezuela’s El Universal criticized for being tamed by mystery new owners.”
92 The competition between the pro-government hashtag #ObamaYankeeGoHome versus the opposition hashtag #ElGobiernoEsLaAmenaza (the government is the threat) is one example of a hashtag dispute that filtered into Twitter’s Trending Topics.
93 Alex Castro, “Futuro Digital Venezuela 2014,” (comScore presentation, Caracas, Venezuela, January 2015) http://bit.ly/1FwDBQ; More than 12 million in Facebook and a little more than 4 million in Twitter are estimated; See also this video for a description of how social media is playing a key role in daily life in Venezuela: “Venezuela: surviving via social media,” *Financial Times* video, 6:26, March 27, 2015, http://on.ft.com/1KOa7XY.
Venezuela

media campaigns. Beginning with a series of protests in February 2014 and continuing through the following year during student and opposition protests, social media has taken on a key role in organizing mobilizations and drawing people out to the street.

In February 2014, local opposition leaders, students, and journalists alike began to turn to social media to organize protests. Thousands of protesters rallied around the hashtags #LaSalida and #12F. During the protests, thousands of people were detained and 43 people were killed in stand-offs between the government and protesters. In the aftermath of the violence, many of the hashtags associated with the protests fell out of use. Protests resurged in May 2015 as people marched for the release of jailed opposition leaders. One opposition leader, Leopoldo Lopez, released a video from his jail cell in which he urged people to protest in the streets, calling for an end to censorship and political persecution, as well as for a date to be set for the upcoming parliamentary elections. The video helped spark a protest on May 30, 2015.

Violations of User Rights

The Venezuelan constitution guarantees freedom of expression, but simultaneously prohibits anonymity. After the massive protests of February 2014, the government cracked down on critical social media users. At least eight social media users were arbitrarily detained during the coverage period. At the same time, the digital sphere has been progressively more restricted through coercive laws and mechanisms of surveillance and control.

Legal Environment

The Venezuelan Constitution guarantees freedom of expression and freedom of speech even while it prohibits anonymity. Despite constitutional protections of free speech, the government has passed a number of laws and regulations that curtail this right online.

In 2010, the National Assembly amended the Law of Social Responsibility in Radio and Television (Resorte-ME) to include regulation over online and electronic media. Vague prohibitions on content under this law provide authorities with sweeping discretion to restrict speech. Article 27, for example, forbids messages that promote anxiety among the population, alter public order, disregard legal authorities, or promote the violation of existing laws. The law also establishes third-party liability for content and requires online media to establish mechanisms to restrict prohibited content. Websites found in violation of these provisions may be heavily fined, and service providers that do not comply risk temporary suspension of operations.

Activists and journalists have also faced charges of defamation under the penal code, which criminal-
izes and sets out prison sentences for defamation against public officials and the publication of false information. Other laws provide additional avenues for limiting speech: for example, the Law of National Security, which was passed in January 2015, outlines prison sentences for individuals who "compromise the security and defense of the nation."

In the past year, high-ranking government officials, including the president and the attorney general, called for further legislation to regulate social media, particularly Twitter. In November 2014, officials in the ruling party introduced legislation to amend the Law on Organized Crime to include crimes for "cyberterrorism." One of the proposed articles would establish penalties for actions against public order that were executed through electronic media or social networks. As of May 2015, the amendment had not yet been passed.

The lack of institutional checks and balances, and in particular the weakness of the judiciary, gives the executive branch significant impunity in monitoring and harassing opponents. The imprisonment of the judge María Afiuni—who had ordered the release of a prominent banker on the grounds that he had been detained beyond the legally allowed time period—demonstrates the pressure faced by the judiciary to comply with political interests. Although the court granted María Afiuni conditional release due to health concerns in December 2014, it prohibited her from using her social media accounts.

### Prosecutions and Detentions for Online Activities

Late 2014 and early 2015 saw a marked increase in arrests of social media users, with everyday users being targeted for seemingly minor infractions. In a period of approximately three months (August-October 2014), security agents detained at least eight people for using Twitter to disseminate facts, images or opinions on social or political topics. Many of the users were arbitrarily detained for long periods of time without due process, and some remain in the custody of the country's intelligence services. In May 2015, the government accused 22 media executives of defamation and banned them from travel outside of the country after three major media outlets republished an opinion piece, originally published in the Spanish newspaper ABC, that accused the president of the National Assembly of drug trafficking.

105 Díaz, "Venezuela: Draft Law Would Criminalize Online Protest, Remove Checks on Surveillance."
107 This was not the only case where the courts ordered a prominent figure to stop using social media accounts after being released from prison. Iván Simonovis, a former security official convicted of involvement in the killing of demonstrators in a 2002 coup, was also prohibited from using social media after he was released to house arrest. "Simonovis no podrá usar redes sociales," El Nacional, September 20, 2014, [http://bit.ly/1rpB3z](http://bit.ly/1rpB3z). For the case of Afiuni, see: "Lawyer: Judge Afiruni has been professionally disabled," El Universal, December 12, 2014, [http://bit.ly/1EKAAdJ](http://bit.ly/1EKAAdJ).
109 Silvia Higuera, “Presidente del Parlamento de Venezuela demanda a medios que replicaron información de diario español,” Blog Periodismo en Las Americas, The Knight Center at the University of Texas Austin, April 23, 2015, [http://bit](http://bit).
Venezuela

One of the most prominent arrests over the past year occurred in February 2014 when the government arrested the major opposition leader Leopoldo López. The government accused López of inciting violence during protests that same month. As evidence in his trial, prosecutors have analyzed over 700 tweets written by López and even accused him of using an online video to spread subliminal messages. Human rights organizations denounced the arrest and pointed out that the government failed to specify how the tweets and videos sent by López led to the actual commission of crimes. In September 2015, López was sentenced to nearly fourteen years in prison.

In October 2014, at least six individuals were arrested for disseminating photographs and information, or simply joking, about the death of Robert Serra, a member of parliament in the ruling party, who was murdered that month:

- Three users were arrested in association with the Twitter account @Hiipolita. On September 24, 2014, Lessi Marcano, who claimed to have abilities to predict the future, tweeted that the National Assembly would be in mourning. When Representative Serra was found stabbed a week later, Marcano was arrested and accused of creating panic and anxiety. Two other users, Ginette Hernández (Marcano’s niece), and Daniely Benítez, were also arrested for alleged connections to the @Hiipolita account. Both Hernández and Marcano remained behind bars as of August 2015.

- Inés Margarita González Árraga (@inesitaterrible) was detained in October 2014 after she published tweets insulting the deceased representative Serra. She was accused of public incitement, violent defamation, and defamation of a public official. In February, she was sentenced to three years in jail.

- Abraham David Muñoz Marchán (@AbraahamDz), an 18-year-old Twitter user, was detained on October 9 for inciting crime for comments he made regarding the death of Deputy Robert Serra, but was later released on probation.

- On October 13, Victor Ugas was arrested for disseminating images of Robert Serra’s corpse, and charged with improper disclosure of data or personal information and digital espionage. He was released in July 2015.

At least two other users were also arrested in the fall of 2014:

- Following the trend of social media users arrested for making predictions, María Magaly

   [ly/1V6Z1cd]; See also “Venezuela court bars media executives from leaving the country,” Committee to Protect Journalists, May 15, 2015, https://cpj.org/x/60J2.


   113 This event occurred outside the coverage period and therefore had no impact on the scores.


Venezuela

Contreras (@marletmaga), a self-described soothsayer, was detained on October 29, 2014 and accused of public incitement and public intimidation after she predicted that there would be water and electricity shortages in the country. She was released after months in detention.118

- Leonel Sánchez Camero (@anonymuswar) was detained on August 22, 2014. He is accused of promoting hatred, conspiring, defamation, and unlawful access to electronic channels due to hacking the Twitter accounts of Jacqueline Faría (Minister of Communication and Information), Gabriela del Mar Ramírez (Ombudswoman), and Eduardo Lima (deputy from the government party, PSUV). He remained detained at the headquarters of the Bolivarian Intelligence Service (SEBIN) at the time of writing this report.119

Out of those still detained, most have not yet been sentenced. Victims of procedural delays, many of them remain detained in the SEBIN headquarters, an intelligence and counter-intelligence body that answers to the Ministry of Internal Affairs, Justice and Peace. The lack of independence in the judiciary is a major concern in these cases. Lawyer Gonzalo Himiob, from the NGO Foro Penal, highlighted that given the nature of their crimes under Venezuelan law, these social media users should have the right to await their trial in freedom.120

Arrests have also occurred as a means to prevent users from recording information that might be embarrassing to the state. In January 2015, 11 people were detained for using their cellphones to take pictures of street protests and the queues in front of supermarkets, but they were immediately released.121 The government has tried to suppress information about the very long queues to buy basic goods in order to avoid publicizing the extent of the economic crisis.

Surveillance, Privacy, and Anonymity

Government surveillance and counterintelligence activities have increased since 2013, when the government released its 2013-2019 Plan for the Homeland, which emphasized the strengthening of national defense among its priorities.122 Although the plan does not explicitly call for the monitoring of social media, after its passage the government began calling for this measure. In October 2013, the president issued a decree creating the Strategic Center for the Security and Protection of the Fatherland (CESPPA), a special body charged with monitoring and tracking of social media and other online information.123 In 2014 the government created the Special Brigade against the Acts of Violent

---

119 Jesús Alberto Yajure, “@Conatel elaboró informes para el @SEBIN_OFICIAL sobre tuiteros detenidos” [@Conatel developed reports for @SEBIN_OFICIAL about the detained Twitter users], July 3, 2015, http://bit.ly/1GXrDwA.
Venezuela

Groups with the goal of gathering coordinating information and activities from all the citizen security and intelligence bodies of the states.124

There are no known cases of government action to restrict information about or access to encryption technologies or other digital tools to ensure the privacy of communications. Furthermore, Venezuelan laws, such as the Law against Cybercrime and the Law to Protect Communication Privacy, guarantee the privacy of communications.125 In practice, however, authorities have failed to apply these laws evenly in cases where activists have sued for protection under the law.126 Although there have been no recent court cases on the matter, the constitution expressly prohibits anonymity.127 In order to buy a cellphone, a SIM card, or a USB modem to access mobile broadband, Venezuelan law requires customers to register using their personal ID number, address, signature, and fingerprints.128

The Law against Kidnapping and Extortion obliges the providers of telecommunications, banking, or financial services to supply data to prosecutors upon presentation of a judicial warrant.129 In practice, given the lack of judicial independence, there are few safeguards in place to limit government security agencies’ access to user data and private communications.

While the full scale of surveillance in Venezuela is unclear, the lack of independent oversight of the country’s media regulator has raised concerns about the ease with which systematic content filtering and surveillance could be implemented. A recent study by Citizen Lab provided evidence that Venezuela is a client of Blue Coat Systems, a computer security company often used by authoritarian governments for monitoring, spying, and censorship of networks.130 Some writers in international media outlets have raised concern about the possibility that a special division within the state-owned ISP CANTV may monitor and track communications.131

Although it is difficult to confirm surveillance, activists have denounced targeted tracking and spying by the government. In 2014, the editor of the digital publication Inside Telecom, William Peña, claimed that state security agents were tracking him because of his critical opinion of the government.132 In May 2015, the Venezuelan NGOs Espacio Publico and Provea denounced government officials for intervening in their private communications after the President of the National Assembly

125 Ley contra los Delitos Informáticos [Law Against Cybercrime], http://goo.gl/VXywPA; Ley Sobre Protección a la Privacidad de las Comunicaciones [Law on Protection of Communications Privacy], http://goo.gl/RPzPYZ.
divulged information on his television show that NGO staff said was only possible to obtain by intercepting private online communications.  

**Intimidation and Violence**

Online journalists, bloggers, and social media activists face harassment in the form of verbal threats, attacks on social media, and potential job loss. Much of the harassment of individuals perceived to be critical of the government does not come directly from the government, but instead from progovernment civilian groups. Although these groups do not necessarily coordinate with the government, they act within an accommodating environment as there are no known cases of state institutions prosecuting a government sympathizer for harassment against a media critic. In fact, government actions sometimes seem to encourage harassment. In March 2015, the president of the National Assembly posted photographs and personal information of human rights activists (including some who work on free expression and digital rights issues) who attended a hearing of the International Assembly of the Human Rights Commission (IAHCR) in Washington D.C. The IAHRC released a public statement criticizing these actions.

Journalists have reported that public officials and members of the media have lost their jobs after expressing controversial opinions on social media. Despite the worrisome precedent set by these layoffs by both public and private agencies, these cases have not been brought to the courts. Online users have also reported a number of instances of harassment via social media networks. The well-known journalist Celina Carquez, who works for the digital media outlet, received threats from unidentified users through Twitter in November 2014. Meanwhile, Carlos Flores, a columnist for the *Huffington Post* and contributor for *Newsweek* in Spanish, denounced profane insults coming from the Twitter account of Tareck El Aissami, the governor of Aragua state.

**Technical Attacks**

Both established and new media outlets that criticize the government have stated that they are...
Venezuela

frequent victims of cyberattack attempts.\(^{140}\) The nonprofit Institute for Press and Society Venezuela released a report showing that 10 percent of members of the media surveyed stated that they had been a victim of illegal interventions (technical attacks) to their email and social media accounts. Although it is suspected that progovernment entities are responsible for the attacks, this has not been confirmed. Also common are technical attacks wherein someone hacks and takes over the Twitter account of an outspoken activist with many followers. \(^{141}\) On the other side, critics of the government have hacked the Twitter account of government officials;\(^{142}\) information sites of the state, such as the National Venezuelan Television\(^{143}\) (VTV by its initials in Spanish), and CANTV.\(^{144}\)


\(^{141}\) Oli-Wan Kenobi, “Usan la app paga para promover una cuenta q usurpa la identidad de @NelsonBocaranda crear confusión y desinformar,” [They use a paid app to promote an account that usurps the identity of @NelsonBocaranda to create confusion and misinform] January 22, 2015. http://goo.gl/tGGR75.


Vietnam

Key Developments: June 2014 – May 2015

- With 29 netizens imprisoned, Vietnam continues to be one of the worst jailers of bloggers in the world (see Prosecutions and Detentions for Online Activities).

- At least eight bloggers were arrested or prosecuted under Article 258 of the penal code for abusing democratic freedom to infringe on state interests (see Prosecutions and Detentions for Online Activities).

- Circular 09 tightened registration and licensing requirements for new social media sites, as well as intermediary liability for third-party content (see Content Removal).

- Decree 174, administering fines for critical content, was widely implemented to punish online speech (see Media, Diversity, and Content Manipulation).
Vietnam

Introduction

The Communist Party was working towards its 2016 party congress during the coverage period of this report. A power reshuffle is anticipated prior to the emergence of a new government. In this environment, repression of critical netizens remained severe. Prisons operated a revolving door policy, with one prominent blogger arrested even as another was released. The period was characterized by ongoing application of Article 258 of the penal code against critics, a trend first noted in Freedom on the Net 2014. Two of the most important critical blogs, Anh Ba Sam, and Que Choa, were blocked, and then stopped operating for most of the coverage period, reducing the diversity and breadth of alternative content.

Administrative fines for critical content, legalized by Decree 174 in 2014, have been increasingly used to threaten media outlets, coupled with disciplinary warnings and job losses. Furthermore, Circular 09 issued in October 2014 made it more difficult for new social media sites to obtain a license and formalized intermediate liability that had been assumed but never codified, though without clear penalties for non-compliance.

Vietnamese activists both in and outside of Vietnam, have long been the target of sophisticated cyberattacks. The malicious software used in the attacks is advanced enough to evade detection by almost all commercial antivirus programs, and sent from servers in locations worldwide. In 2015, cyberattacks became more personalized, indicating that attackers are familiar with the activities and interests of their targets.

Obstacles to Access

Internet penetration is comparatively high, and almost universal among urban youth, due to low cost and high availability in semi-public spaces. Investment is still needed to improve speed, and the infrastructure is vulnerable to physical damage. The telecom market is dominated by a few players, most of them state-owned, lacking fairness and autonomy by international standards.

Availability and Ease of Access

Internet access continued to increase during the coverage period of this report, with penetration reaching 44 percent in 2014, up from 39 percent in 2013. Vietnam ranked 101 on the global ICT Development Index in 2013, higher than regional neighbors with a larger gross domestic product like Indonesia and the Philippines.

However, internet speed is among the lowest in Asia Pacific, having fluctuated during previous quarters. High speed broadband adaption reached 22.4 millions subscribers, or about 40 percent of Internet users, an 11 percent increase from 2012.

---

Vietnam

Vietnam's mobile penetration was estimated at 147 percent in 2014, indicating some users have more than one device or SIM card. Fifty-six percent of users accessed the internet via a mobile device in 2012, almost double the number in 2011. The growth of mobile phone penetration slowed somewhat in recent years, as new policies discouraged people from buying new SIM cards. Despite this, the 3G network operating since 2009 is growing fast. As of October 2013, Vietnam has 19 million 3G users, up from 3 million in 2011. Vietnam still has no strategy to introduce a 4G network.

Vietnam does not report figures for computer literacy, but the literacy rate at 93 percent has helped equip the adult population to use computers. Wi-Fi connections are free in many urban spaces such as airports, restaurants, and hotels, and city-wide in some tourist destinations. Access via smartphones has increased, being the choice for 36 percent of internet users, compared to 44 percent who use a PC.

While access is more limited for 70 percent of the population living in rural areas, with ethnic minorities and remote, impoverished communities especially disadvantaged, a remarkable 95 percent of citizens aged 15 to 24 nationwide have some degree of internet access. Monthly wired access has decreased, starting at around US$9 per month, which is considered affordable in cities, and pay-per-use wireless packages are even more affordable, though less reliable.

Restrictions on Connectivity

While several companies have licenses to build infrastructure, military-owned Viettel, state-owned Vietnam Post and Telecommunications (VNPT), or their subsidiaries, are the dominant equipment providers in practice. VNPT operates the national-level backbone network. Four out of six internet exchange providers, which operate the internet exchange points (IXPs) and allow ISPs to interconnect, are state- or military-owned. Although this suggests a concerning degree of state influence over the internet architecture, authorities in Vietnam did not employ noticeable throttling or restrict access to the internet for political reasons during the coverage period of this report, though such interference has been suspected in the past. Connections suffered when the Asia-America Gateway (AAG) submarine cable, one of several which carry international traffic, was damaged. In 2014 the cable was disconnected twice. In May 2015, the latest damage impacted Internet availability and speed for two weeks. Such outages are frequent and significantly impair the speed and quality of access.

ICT Market

The three biggest internet service providers (ISPs) are the state-owned VNPT, which controls 51 percent of the market; Viettel (40 percent); and the private FPT (6 percent). VNPT and Viettel also own the three largest mobile phone service providers in the country (MobiFone, VinaPhone, and Viettel),
Vietnam

which serve 93 percent of the country’s 2G and 3G subscriber base, while two private companies share the remainder.¹² Though any firm is allowed to operate an ISP, informal barriers prevent new companies without political ties or economic clout from disrupting the market.

Regulatory Bodies

The Vietnam Internet Center (VNNIC) allocates internet resources such as domain names under the Ministry of Information and Telecommunication. Three additional ministries—information and culture (MIC), public security (MPS), and culture, sport, and tourism (MCST)—manage the provision and usage of internet services. On paper, the MCST regulates sexually explicit and violent content, while the MPS oversees political censorship. In practice, however, guidelines are issued by the VCP in a largely non-transparent manner. In 2008, the MIC created the Administrative Agency for Radio, Television, and Electronic Information. Among other duties, the agency is tasked with regulating online content, which includes drafting guidelines for blogs and managing licenses for online media.¹³

Limits on Content

Political content on a range of sensitive topics is restricted online, especially in Vietnamese. Decree 174, effective since January 2014, was widely used during the coverage period to levy harsh fines for government criticism on online media. Additionally, Circular 09, issued in October 2014, requires website owners to respond immediately to authority’s request to take down content resulting in increased self-censorship. Commentators paid and officially acknowledged by the government in 2013, have grown in number and continue to manipulate online content.

Blocking and Filtering

With fewer resources devoted to online content control than in China, the Vietnamese authorities have nevertheless established an effective content filtering system. Censorship is implemented by ISPs rather than at the backbone or international gateway level. No real-time filtering based on keywords or deep-packet inspection has been documented. Instead, specific URLs are identified in advance as targets for censorship and placed on blacklists. The authorities are not known to have instituted restrictions on email or SMS content.

Blocking in Vietnam primarily targets topics with the potential to threaten the Vietnam Communist Party’s (VCP) political power, including political dissent, human rights and democracy, as well as websites criticizing the government’s reaction to border and sea disputes between China and Vietnam. Content promoting organized religion such as Buddhism, Roman Catholicism, and the Cao Dai group, which the state considers a potential threat, is blocked to a lesser but still significant degree. Vietnamese sites critical of the government are generally inaccessible, whether they are hosted overseas, such as Talawas, Dan Luan, and Dan Chim Viet, or domestically, like Dan Lam Bao, Dien Dan Xa Hoi Dan Su or Bauxite Vietnam.

ISPs use different techniques to inform customers of their compliance with blocking orders. While

¹² “Việttel dẫn đầu về di động, VNPT chiếm lĩnh thị phần Internet băng rộng,” [Viettel leads in mobile, VNPT gains in broadband market].
Vietnam

some notify users when an inaccessible site has been deliberately blocked, others post an apparently benign error message. Censors largely focus on Vietnamese-language content, so the New York Times and Human Rights Watch websites are accessible, while the U.S.-funded Radio Free Asia’s Vietnamese-language site is not; similarly, BBC websites are accessible in English but not Vietnamese. Blocking is not consistent across ISPs. A 2012 OpenNet Initiative test of 1,446 sites found Viettel blocked 160 URLs, while FPT blocked 121, and VNPT only 77. There is no avenue for managers of blocked websites to appeal censorship decisions.

Content Removal

The party’s Department for Culture and Ideology and the MPS regularly instruct online newspapers or portals to remove content they perceive as problematic, through nontransparent internal, mostly verbal orders.

Intermediary liability has long been implied in Vietnam, but was formalized in 2013 with Decree 72 on the Management, Provision, Use of Internet Services and Internet Content Online. It requires intermediaries—including those based overseas—to regulate third-party contributors in cooperation with the state, and to “eliminate or prevent information” prohibited under Article 5. It holds cybercafe owners responsible if their customers are caught surfing “bad” websites. This process was articulated in Circular 09/2014/TT-BTTTT, issued in October 2014, which requires website owners to eliminate “incorrect” content “within three hours” of its detection or receipt of a request from a competent authority in the form of email, text message, or phone call. The circular also tightened procedure for registering and licensing new social media sites.

It is not clear how much service providers removed content for fear of possible reprisals before the decree was introduced, so its immediate impact was not possible to gauge. Further, it did not outline what penalties non-compliant companies could face, and how the decree might be enforced remains unclear.

Media, Diversity, and Content Manipulation

Internet content producers face a range of pressures that affect the quality of online information. All content needs to pass through in-house censorship before publication. Editors and journalists also risk post-publication sanctions including disciplinary warnings, job loss, or imprisonment. In weekly meetings, guidelines are handed out by a Party Committee to editors about areas and themes to report on or to, as well as the allowed depth and breadth of coverage.

Decree 174, effective since January 2014, introduced administrative fines of VND 100 million (US$4,700) for anyone who “criticizes the government, the Party or national heroes” or “spreads propaganda and reactionary ideology against the state” on social media. These can be applied to offenses not serious enough to merit criminal prosecution. The decree outlined additional fines

15 Poetranto, “Update on Threats.
16 Poetranto, “Update on Threats.
Vietnam

for violations related to online commerce. During the coverage period, Decree 174 has been used heavily. In February 2015, newspaper Nguoi Cao Tuoi received a total fine of about US$35,000 for several offenses.

These economic and social penalties, in addition to the risk of criminal prosecution, foster self-censorship. The unpredictable and nontransparent ways in which topics become prohibited make it difficult for users to know what might be off-limits, and bloggers and forum administrators routinely disable commenting functions to prevent controversial discussions.

Despite government restrictions, Vietnam’s internet is vibrant and offers a diversity of Vietnamese-language content. Although most content addresses personal and apolitical topics, citizen journalism has emerged as an important source of information for many Vietnamese, particularly given the tightly controlled traditional media. People now recognize the parallel existence of official media and alternative counterparts operating exclusively online. In large cities, the internet has surpassed newspapers as the most popular source for information. In some cases such as the workers’ riots in Binh Duong province protesting a Chinese oil rig in the East China Sea in May 2014, Facebook users broke news faster and in more detail than mainstream media outlets restricted by tighter censorship.

YouTube, Twitter, and international blog-hosting services such as Blogger or WordPress are freely available and growing in popularity, although Twitter is used to a lesser extent than in some other Asian countries. Tools for circumventing censorship are well-known among younger, technology-savvy internet users in Vietnam, and many can be found with a simple Google search. Facebook, which faced sporadic—and officially unacknowledged—blocks in 2010 and 2011, was largely accessible and popular in 2015. Government agencies, such as the Ministry of Health, have started to reach out to citizens on Facebook, apparently signaling a shift away from the perception of such platforms as oppositional towards more digital engagement in combination with selective repression and blocking of contents, for propaganda purposes.

The government has also taken steps to manipulate public opinion online. In 2013, Hanoi’s Propaganda and Education Department revealed that it runs at least 400 online accounts—without specifying what type—and 20 microblogs to fight “online hostile forces.” On March 14, 2015, alleged progovernment commentators insulted online activists and hindered them as they gathered offline to commemorate a battle against China although the Hanoi’s government denied that these people are under their management. Some blogs which criticize high-profile party members, such as Quan Lam Bao in 2013, or Chan Dung Quyen Luc in 2014, have attracted accusations that they reflect internal power dynamics rather than objective opinion. As such, critics say, they contribute little to the cause of freedom of expression.

Vietnam

Digital Activism

While important blogs such as Anh Ba Sam and Que Choa stopped operating during most of the coverage period due to the arrest of their owners, the easy accessibility of Facebook provided people with opportunities to engage in social activism and share reactions to socio-political events. However, digital mobilization is local rather than national in scale, compared to some other countries in Asia. In 2012, blogs played an important role in rallying public opinion and providing evidence against local authorities who seized agricultural land from farmers.25 In 2013, LBGT activists used social media to show support for same-sex marriage.26 Most recently, in March 2015, social media provided the space for public outcry and helped to organize citizen’s protest against the Hanoi government’s large-scale deforestation plan, and eventually brought it to a halt.27

Violations of User Rights

The interrogation, imprisonment, and physical abuse of bloggers and online activists, which intensified in 2013, continued during the coverage period. Harsh sentences are handed down in cursory trials often closed to the public and press. In late 2014 and early 2015, Article 258 of the penal code was used to convict at least 10 rights advocates and arrest 4 bloggers. Hackers have targeted Vietnamese anti-government activists since 2009. During the past year, cyberattacks got more personal with campaigns designed to suppress criticism and diversified their targets.

Legal Environment

The constitution, amended in 2013, affirms the right to freedom of expression, but in practice the VCP has strict control over the media. Legislation, including internet-related decrees, the penal code, the Publishing Law, and the State Secrets Protection Ordinance, can be used to fine and imprison journalists and netizens. The penal code’s notorious Articles 79 and 88 are commonly used to prosecute and imprison bloggers and online activists for subversion and propaganda against the state.28 Article 258, which punishes “abuse of democratic rights to infringe upon the interests of the State, the legitimate rights and interests of organizations and citizens,” is also increasingly being used to arrest bloggers. The judiciary is not independent, and trials related to free expression are often brief, and apparently predetermined. Police routinely flout due process, arresting bloggers and online activists without a warrant or retaining them in custody beyond the maximum period allowed by law.

Since 2008, a series of regulations have extended controls on traditional media content to the online sphere, starting with Decree 97 which ordered blogs to refrain from political or social commentary and barred them from disseminating press articles, literary works, or other publications prohibited by the Press Law.29 Decree 02 followed in 2011, giving authorities power to penalize journalists and

---

Vietnam

bloggers for a series of infractions, including publishing under a pseudonym. The decree differenti-
ated between journalists accredited by the government and independent bloggers, who are allowed
far fewer rights and protections.\(^{30}\)

Decree 72 on the Management, Provision, Use of Internet Services and Internet Content Online,
which came into effect in September 2013 and replaced Decree 97 of 2008, prolonged this repres-
sive trend of replacing “blogs” with “social networks” to encompass more online platforms.\(^{31}\) Article 5
limits overbroad categories of online activity including “opposing the Socialist Republic of Vietnam,”
inciting violence, revealing state secrets, and providing false information.

In October 2014, The Ministry for Information and Telecommunication issued Circular 09/2014/TT-
BTTTT, which tightens the management of social networks, mostly through tougher requirements for
licensing and registration. Among others, the person responsible for the platform should now have a
university or higher degree. The website should have a “regime for elimination of incorrect contents
within three hours from its detection or the request of a competent authority in the form of email,
text or phone.”\(^{32}\)

**Prosecutions and Detentions for Online Activities**

According to Reporters Without Borders, 29 netizens were imprisoned in Vietnam as of December
2014, compared to 17 in 2011, making the country one of the world’s worst jailers of bloggers and
internet users.\(^{33}\) The increase was fueled by a 2013 court ruling that found 14 Catholic students,
bloggers, and human rights activists guilty of subversion under Article 79, in part for their online ac-
tivities.\(^{3435}\) The sentences ranged from 3 years in prison followed by 2 years under house arrest to 13
years’ imprisonment and 3 years’ house arrest.\(^{36}\)

In 2014, Vietnamese authorities used Article 258 to convict at least 10 rights advocates and arrest 4
bloggers.\(^{37}\) Examples during the coverage period include:

- Prominent blogger Nguyen Huu Vinh, who writes Anh Ba Sam, and his collaborator, Nguyen
  Thi Minh Thuy, were arrested on May 5, 2014, for publishing online articles which “abuse
democratic freedoms to infringe on the interests of the state.”\(^{38}\)

- On June 26, 2014, the Supreme People’s Court in Danang upheld a two-year prison sen-

---

Vietnam

tence handed down in March 2014 against blogger and former journalist Truong Duy Nhat for publishing critical articles on his blog “A Different Point of View.” The blogger has been detained since his arrest in May 2013.39

- Nguyen Quang Lap, the well-known writer and owner of Que Choa, one of Vietnam’s most visited political blogs, was arrested on December 6, 2014. A week earlier, Hong Le Tho, another independent blogger, was arrested in Ho Chi Minh City. Both were charged with “abusing democratic freedoms.”40 Nguyen Quang Lap was released on February 11, 2015, but the charges were not dropped.

- On February 12, 2015, a provincial court in Dong Nai sentenced three bloggers, Le Thi Phuong Anh, Do Nam Trung and Pham Minh Vu, who were arrested in May 2014 while covering anti-Chinese protests by workers. They received between 12 and 18 months in prison each for using Facebook to “disseminate content that incited and led to anti-state demonstrations.”41

- On 12 May 2015, Kim Quoc Hoa, former editor in chief of the mainstream print and online newspaper Nguoi Cao Tuoi, was prosecuted for “abusing democratic freedoms to infringe on the state’s interest. Three months earlier, he lost his job and the online version of the newspaper was forced to shut down.42

Arrests and sentences were also documented on other charges:

- On August 26, 2014, a court in the province of Dong Thap sentenced blogger and activist Bui Thi Minh Hang to three years in prison, and her co-defendants, religious workers Nguyen Van Minh and Thi Thuy Quynh, to 30 and 24 months respectively. All three were convicted of “causing public disorder” in public under Article 245 of the penal code. At the trial police prevented 200 people, including friends and relatives, from attending, and arrested 40 supporters of the defendants.43

- Nguyen Dinh Ngoc, another well-known blogger who writes under the pen name Nguyen Ngoc Gia, was arrested in his home in Ho Chi Minh City on December 27, 2014, for illegal activities, with no specific charge given.44

Photo journalist Dang Nguyen Minh Man, arrested four year ago and currently serving an eight year prison term with four subsequent years of house arrest for committing “activities aimed at overthrowing the government” has been on hunger strike for prolonged periods to protest the ill-treatment she has received while in detention. Minh Man’s treatment is not exceptional. Amnesty International noted in a 2013 report many political prisoners were held in harsh conditions that amounted to cruel, inhumane or degrading treatment.45

---

Surveillance, Privacy, and Anonymity

Limited information is available about advanced surveillance technology available to Vietnamese authorities. In 2013, Citizen Lab, a research group based in Canada, identified FinFisher software on servers in 25 countries worldwide, including Vietnam. Promoted by United Kingdom-based distributor Gamma International as a suite for lawful intrusion and surveillance, FinFisher offers the power to monitor communications and extract information without permission from other computers, such as contacts, text messages, and emails. Citizen Lab noted that the presence of such a server did not prove who was running it, though it is marketed to governments.

Decree 72 requires providers like social networks to “provide personal information of the users related to terrorism, crimes, and violations of law” to “competent authorities” on request, but lacks procedures or oversight to discourage intrusive registration or data collection. It also mandates that companies maintain at least one domestic server “serving the inspection, storage, and provision of information at the request of competent authorities.” The decree gave users themselves the ambiguous right to “have their personal information kept confidential in accordance with law.” Implementation is at the discretion of ministers, heads of ministerial agencies and governmental agencies, the provincial People’s Committees, and “relevant organizations and individuals”, leaving anonymous and private communication subject to invasion from almost any authority in Vietnam in the future. There has been no known case where the Decree was applied so its consequences are unknown.

Real-name registration is not required to blog or post online comments, and many Vietnamese do so anonymously. However, Vietnamese authorities do monitor online communication and dissident activity. Cybercafe owners are required to install software to track and store information about their clients’ online activities, and citizens must also provide ISPs with government-issued documents when purchasing a home internet connection. In late 2009, the MIC requested all prepaid mobile phone subscribers register their ID details with the operator and limited each to three numbers per carrier. As of 2015, however, the registration process is not linked to any central database and could be circumvented using a fake ID. Pay-per-use, called “throw away” or “one off” SIM cards, can be easily purchased without IDs.

Intimidation and Violence

In addition to imprisonment, bloggers and online activists have been subjected to physical attacks, job loss, severed internet, travel restrictions, and other rights violations. On November 2, 2014, former prisoner of conscience and freelance journalist Truong Minh Duc was ambushed and beaten until he lost consciousness by eight police officers in plain clothes, the third of such incidents target-
Vietnam

ing rights campaigners within a two month period. In January 2015, 12 bloggers and right activists were assaulted by anonymous thugs as they were visiting a fellow activist.

On April 30, 2015, the 40th anniversary of the end of the Vietnam War, bloggers and activists were placed under close surveillance, subjected to intimidation and, in some cases, assaulted. House arrest measures were reinforced; independent reporters—including Pham Chi Dung, who is on the Reporters Without Borders list of “information heroes”—were prevented from covering the celebrations. Finally, on May 11, 2015, blogger and activist Nguyen Chi Tuyen, most recently active in protests against government’s tree felling in Hanoi, was beaten brutally by thugs, hospitalizing him.

Technical Attacks

Activists in Vietnam and abroad have been the target of systematic cyberattacks. When activity was first documented in 2009, the attackers used Vietnamese-language programs to infect computers with malicious software to carry out distributed denial-of-service (DDoS) attacks on blogs and websites perceived as critical of the government. Google estimated that “potentially tens of thousands of computers” were affected, but Vietnamese authorities took no steps to find or punish the attackers.

Activists today are subject to account takeovers, where spear-phishing emails disguised as legitimate content carry malware which can breach the recipient’s digital security to access private account information. In 2013, attackers seized control of a handful of important alternative blogs, including websites Anh Ba Sam, Que Choa, and blogs written by activists Xuan Dien, Huynh Ngoc Chenh, and others. It is common for sites to post a list of alternative URLs in case the current one is hacked.

Starting in 2013, attacks using malware to spy on journalists, activists and dissidents have become more personal. California-based Electronic Frontier Foundation (EFF) and Associate Press journalists have received infected emails inviting them to human rights conferences or offering academic papers on the topic, indicating that the senders are familiar with the activities and interest of the receivers. According to EFF’s analysis, the detection rate for the malware is very low - only one anti-virus vendor out of a possible 47 could detect it as of January 2014. In 2015, targeted personalized attacks were reported by several internet professionals in Vietnam.

61 Personal interviews, 2015.
Zambia

Key Developments: June 2014 – May 2015

- There were no websites blocked during the coverage period, compared to the previous period, when four independent news outlets were targeted for blocking (see Blocking and Filtering).

- Despite the unblocking of critical websites, government officials repeatedly issued threats to shutdown select websites and blogs (see Blocking and Filtering).

- Leaked emails from the Italian surveillance firm Hacking Team revealed that the company may have sold its sophisticated spyware known as Remote Control System (RCS) to the Zambian authorities (see Surveillance, Privacy, and Anonymity).
Zambia

Introduction

Zambia was among the early adopters of the internet in sub-Saharan Africa with the installation of dial-up and satellite technology at the University of Zambia in the early 1990s. It was also incidentally one of the first countries in the region to censor online content. In 1996, the government demanded the removal of a banned edition of The Post from the newspaper’s website by threatening to hold the internet service provider (ISP), Zamnet, criminally liable for the content. There were no other reported incidents of internet censorship until July 2013, when four independent online news outlets were blocked, purportedly by the government for their critical coverage of the Patriotic Front (PF) ruling party under President Michael Sata.

In 2014-2015, the Zambian government eased up on earlier efforts to restrict internet freedom, which included the blocking of news websites from July 2013 to April 2014 and arrests of several journalists suspected of their affiliation with the blocked news outlets. This continued under the new president, Edgar Lungu, who was elected in January 2015 in a presidential by-election following the death of President Michael Sata in October 2014. Nevertheless, government officials repeatedly issued threats to shutdown select websites and blogs throughout the year, and the blocking of critical websites in the past suggests that this method of internet censorship may be practiced again in the future.

Concerns of government surveillance increased in 2015, particularly after leaked emails from the Italian surveillance firm Hacking Team revealed that the company may have sold its sophisticated spyware known as Remote Control System (RCS) to the Zambian authorities.

Obstacles to Access

Internet and mobile access rose steadily though remained low, hindered by high costs, poor infrastructure, and a large urban-rural divide.

Availability and Ease of Access

Access to information and communication technologies (ICTs) in Zambia has increased steadily over the past few years, from a penetration rate of 10 percent in 2010 to over 17 percent in 2014, according to the International Telecommunication Union (ITU).1 However, mobile phone penetration increased more rapidly, growing from 49 percent in 2010 to 67 percent in 2014 as most Zambian ICT users access the internet via mobile phones.2 As of March 2015, mobile internet users comprise 28 percent of the Zambian population, increasing from a mere 3 percent in 2011.3 Meanwhile, internet connection speeds in Zambia are slow, averaging 1.3 Mbps compared to a global average of 3.9 Mbps, according to May 2015 data from Akamai’s State of the Internet report.4

The costs of ICT ownership and access are very expensive and out of reach for the majority of citizens in Zambia, where the average minimum wage is approximately US$75 per month. Blackberry

---

Zambia devices are the most popular internet-enabled mobile phones in Zambia due to cheap subscription fees, which cost as low as US$10 per month for access. Nevertheless, high costs hinder most Zambians from accessing more advanced internet applications, with a standard smart phone costing about US$250 while broadband subscriptions cost an average of US$50 for a 10 GB of data. Less than 1 percent of Zambians access the internet from their homes via fixed-line broadband subscriptions, which cost an average of US$62 as of February 2015. Zambians also access the internet at cybercafes, which cost slightly less than US$2 per hour. In recent years, however, cybercafes have become less popular as people increasingly access the internet via mobile devices.

While access to ICTs is steadily increasing, it is only widespread in urban areas such as Lusaka (the capital), Copperbelt (the economic hub of the country), and Livingstone (the tourist capital). Access in rural areas has lagged behind due to the high costs of hardware and software, erratic and expensive electricity, poor network coverage, and high levels of illiteracy. Moreover, the government has lacked the resources needed to prioritise the development of ICT infrastructure in rural areas, resulting in a significant urban-rural divide.

Restrictions on Connectivity

There have been no reports of the Zambian government restricting connectivity to internet or mobile phone services to date, though partial state ownership over the country’s fiber backbone and control over connections to the international internet may enable the government to restrict connectivity at will.5

As a landlocked country, Zambia’s national fiber backbone is provided by three operators: state-owned Zambia Telecommunications Ltd (Zamtel), state-owned Zambia Electricity Supply Corporation Ltd (ZESCO),6 and privately-owned Copperbelt Energy Corporation (CEC). Zamtel operates the fiber-optic connection to two international submarine cables the WACS and Sat-3.7 MTN and Airtel lease access to the undersea cables from Zamtel, while MTN also connects directly to the EASSy.8 According to a July 2013 Zambian Watchdog report, the government may also control the country’s internet exchange point (IXP), which is reportedly housed in the same building as state-owned Zamtel in Lusaka.9

ICT Market

The Zambian market for ISPs is very competitive and characterized by a lack of a significant dominant player.10 As of 2015, there are 23 ISPs, three of which are also the country’s mobile phone pro-

---

Providers: MTN, Airtel, and state-owned Zamtel. All internet and mobile service providers are privately owned, with the exception of Zamtel, which was renationalized in January 2012 under the directive of the late President Michael Sata. Sata’s predecessor had sold the 75 percent share of Zamtel to Lap Green in 2010 for US$257 million. While Zamtel has the smallest share in the mobile phone market, it commands the largest share of internet subscriptions, with 61 percent of the market, as of February 2013.

Regulatory Bodies

The Zambia Information and Communications Authority (ZICTA) is the regulatory body for the country’s ICT sector. Established under the Information and Communication Technologies Act of 2009, ZICTA is known to be generally autonomous in its decision-making, although the government has some ability to influence ZICTA’s activities. The Minister of Information and Broadcasting Services is mandated to oversee ZICTA’s activities and appoint the members and chairperson of the ZICTA board. The minister is also entitled to issue general directives, which the regulator is obligated to carry out.

Some internet content is also regulated by the Independent Broadcasting Authority, which oversees the enforcement and compliance of regulations in broadcast programming. This includes programming that is streamed and published online by TV and radio stations.

Limits on Content

Online content in Zambia was unrestricted during the coverage period, in contrast to the previous period when four independent online news outlets were blocked for several months.

Blocking and Filtering

In 1996, Zambia became the first country in sub-Saharan Africa to censor online content when the government demanded the removal of a banned edition of The Post from the newspaper’s website by threatening to hold the internet service provider (ISP), Zamnet, criminally liable for the content. There were no other reported incidents of internet censorship until July 2013, when four independent online news outlets—Zambia Watchdog, Zambia Reports, Barotse Post, and Radio Barotse—were blocked until April 2014, purportedly by the government for their critical coverage of the Patriotic

---

13 Matthew Saltmarsh, “Privitization of Zambian Phone Company Degenerates Into a Feud,” *New York Times*, October 3, 2010, [http://nyti.ms/1VURg8z](http://nyti.ms/1VURg8z).
16 International Telecommunication Union, “Zambia Profile (Latest data available: 2013).”
17 First Schedule (Section 4), The Information and Communication Technologies Act [No. 15 of 2009].
Zambia

Front ruling party under President Michael Sata. The government had previously tried to ban Zambian Watchdog in 2012.

No other websites were blocked during the coverage period; social media and communications platforms such as YouTube, Twitter, Facebook, WhatsApp, and international blog hosting services were freely available. Nevertheless, government officials repeatedly issued threats to shutdown select websites and blogs, and the 2013-2014 blocking of critical news websites suggests that this method of internet censorship may be practiced again in the future.

There is no concrete evidence that the government was behind the blocking of websites in 2013 and 2014, indicating a complete lack of transparency behind censorship decisions, in addition to an ineffective complaints and appeals process through the regulatory body ZICTA. Testing conducted by the Tor Project’s Open Observatory of Network Interference (OONI) in July 2013 discovered the presence of deep packet inspection (DPI) filtering tactics as the source of the block. Zambian Watchdog accused Chinese company Huawei Technologies of installing DPI on Zambia’s ISPs to enable the blocking of internet content. While the government did not claim responsibility for the blocking, Vice President Guy Scott reportedly stated that the independent outlet deserved to be censored because it was “promoting hate speech” and disseminating false news. He also characterized the party responsible for the blocking as a “well-wisher” and thanked them for their work.

Content Removal

The government has also been known to censor internet content by directing online media editors to remove material considered problematic or offensive upon request. However, the extent of this practice is unknown given the predominance of state-owned and progovernment news outlets in the country. Instances of takedown requests are likely unreported, while self-censorship may limit the volume of critical content that could be targeted. The only known incident comes from Zambia Reports, who publicly admitted to complying with a government takedown request in its July 2013 open letter to the government, though the outlet did not reveal the nature of the content that was taken down or when it occurred.

Otherwise, intermediaries are not held liable for content under the 2009 Electronic Communications and Transactions Act.

Media, Diversity, and Content Manipulation

Online content producers face considerably less government pressure compared to their traditional media counterparts, though the majority of online news sources in Zambia are merely web versions of progovernment mainstream outlets. As a result, social media platforms and citizen journalists

---

have emerged as important sources of information, and Zambians now recognize the parallel existence of official media and alternative voices from online sources. The Zambian blogosphere is vibrant, representing diverse viewpoints and opposition voices, and many mainstream journalists have turned to blogs to express themselves more freely. Zambia's internet offers content in five local languages, including English, although it is difficult to find content produced or written strictly in local languages.

While blogs hosted on international platforms have proliferated in recent years, online publications face economic constraints that compromise their ability to remain financially sustainable. The government is the largest source of advertising revenue for traditional media outlets and has been known to withhold advertisements from critical outlets. Moreover, private companies often do not advertise in news outlets that seem antagonistic to government policies out of fear of the potential repercussions. These trends are likely mirrored online, though in general, online news platforms are much less developed than print and broadcast media. The two most popular independent online news outlets in Zambia—Zambian Watchdog and Zambia Reports—are both hosted abroad and receive advertising revenue from international businesses.

Growing government pressure on the media in recent years has created a climate of self-censorship among journalists, both on and offline. Online journalists and bloggers are increasingly choosing to write anonymously due to harassment, the threat of legal action, or both, particularly on issues regarding politics and corruption involving government officials. Social media users tend to express themselves more freely online, but a growing belief that the government monitors social media activity has made users more cautious in recent years. Meanwhile, progovernment trolls are becoming increasingly common on social media platforms such as Facebook, typically flooding posts that are critical of the government with insults and comments on unrelated issues. Some observers suspect that the government may be paying the trolls to disseminate progovernment propaganda.

Digital Activism

Social media outlets, particularly Facebook, have played an important role in mobilizing Zambian citizens around a variety of social and economic issues, such as land reform, the mining industry, and taxes. Digital activism efforts have yet to result in significant social or political change. In 2014, the poverty alleviation organization Action-Aid Zambia led a social media campaign to lobby for reform and transparency in the country’s mining taxation laws, persuading the Zambian government to begin a review some of the contentious laws governing the mining sector.

---

Violations of User Rights

The Zambian government was less restrictive on online journalists during this report’s coverage period compared to the previous period, when the authorities used both legal and extrajudicial measures to punish online journalists for critical media coverage. No arrests for online activities were reported, while one journalist arrested in 2013 was acquitted of all charges. Leaked emails from the Italian surveillance firm Hacking Team revealed that the company may have sold its sophisticated spyware known as RCS to the authorities.

Legal Environment

Freedom of expression is enshrined in the Zambian Constitution but is limited by broad interpretations of other statutes that restrict expression in the interest of public order and safety, national security, morality, and health. The constitution does not explicitly guarantee press freedom but includes a provision stating, “no law shall make any provision that derogates from freedom of the press.” Some media observers have noted that the provision inadequately protects press freedom. However, a new draft constitution was posted online for public review in October 2014. The draft constitution includes specific protections for print, broadcast, and electronic media freedom, and explicitly prohibits the government from exercising control or interfering with media activities. As of mid-2015, the review process for the draft constitution was still ongoing.

Nevertheless, freedom of expression and the media continue to be limited by clauses in the penal code that criminalize defamation of the president and give the president “absolute discretion” to ban publications regarded as “contrary to the public interest.” In April 2014, the government reportedly stated intentions to introduce legislation regulating online media, citing the problems of “internet abuse” and cybercrime. To date, no restrictive laws related to the regulation of ICTs and online activities have been introduced.

Judicial independence is guaranteed in the constitution but in practice this is not respected and undermined by other laws that allow for executive interference in Zambia’s justice system. Notably, the Service Commissions Act—which establishes a Judicial Service Commission to advise the president on judicial appointments—provides the president with the power to give the commission “general directions as the President may consider, necessary” and obliges the commission to comply with the directions.

---

43 The Penal Code Act, Chapter 7, art. 53.
Zambia

Prosecutions and Detentions for Online Activities

The Zambian government was less restrictive on the press and Zambian internet users during this report’s coverage period compared to the previous period, when the authorities used both legal and extrajudicial measures to punish online journalists for critical media coverage. In 2013, three journalists suspected of working for Zambian Watchdog were arrested and handed trumped up charges of sedition and possession of obscene material. In August 2015, one of the journalists, Clayson Hamasaka, who was charged with possession of pornography, was acquitted after a court ruled that the evidence against the journalist had been planted. The other two cases were still in the courts awaiting judgments as of October 2015, and no arrests for online activities were reported from June 2014 to May 2015.

Surveillance, Privacy, and Anonymity

Little is known about the Zambian government’s surveillance practices and capabilities. In July 2015, email leaks from the Italian surveillance firm Hacking Team revealed that the company may have sold sophisticated spyware known as Remote Control System (RCS) to the Zambian authorities. While the leaked emails did not confirm the sale, they point to the government’s intent to acquire such technologies that can monitor and intercept user communications.

The Electronic Communications and Transaction Act of 2009 details conditions for lawful interception of communications, which generally requires a court order. Yet, under the late President Michael Sata, numerous reports accused the government of conducting extensive illegal surveillance of citizens’ ICT activities, such as the phone tapping of senior government officials who fell out of the ruling party’s favor, civil society leaders, and journalists.

Otherwise, details of potential extralegal government surveillance stem mostly from Zambian Watchdog reports. According to the news outlet, the government contracted Chinese experts in 2013 to install an internet surveillance system that could monitor, intercept, censor, and mine data from digital communications. The subsequent blocking of Zambian Watchdog and Zambia Reports in July 2013 corroborated the use of deep-packet inspection (DPI) technology as the mechanism behind the blocking. Zambian Watchdog also separately reported that President Sata had signed a

---

54 Many of Zambian Watchdog's news reports about surveillance could not be corroborated by a second source.
56 OONI, “Zambia, a country under Deep Packet Inspection.”
presidential order in February 2013 authorizing the president’s office to interfere with ICT communications without oversight.⁵⁷ According to the anonymous news article, ZICTA had directed all ISPs and mobile service providers in Zambia “to allow safe passage of Information Technology (IT) Specialists from the Office of the President and China.”⁵⁸ Later in September 2013, Zambian Watchdog reported that China’s Huawei had installed email hacking devices on all ISPs in Zambia.⁵⁹ No further reports of surveillance abuse have been reported under Zambia’s new president, Edgar Lungu, elected in January 2015.

The ability for Zambians to communicate anonymously through digital media is compromised by SIM card registration requirements instituted in September 2012.⁶⁰ Registration requires an original and valid identity card such as a national registration card presented in person to a registration agent at a mobile service provider.⁶¹ While the government stated that the registration requirements were for the purposes of combatting crime,⁶² Zambian Watchdog reported a story in November 2012 based on inside sources alleging that subscriber details were passed directly to the secret service for the creation of a mobile phone user database.⁶³ An official from ZICTA also publicly stated in November 2012 that registration would “enable law enforcement agencies [to] create a database to help identify the mobile SIM card owners,” according to a news report in Lusaka Times.⁶⁴

Registration for the .zm country code top-level domain (ccTLD) is managed by ZICTA as provided for under the 2009 Electronic Communications and Transaction Act, which may compromise the anonymity of .zm website owners given the murky independence of the regulatory authority.⁶⁵ The act also provides a government minister the authority to create statutory agreements that determine further requirements for domain name registration, in addition to “the circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked.”⁶⁶ Such direct oversight of local web domains may allow the government to access user data belonging to local content creators and hosts.

**Intimidation and Violence**

In the past few years, journalists have noted an increased climate of intimidation for media workers who regularly face harassment and physical attacks for their independent reporting. While there were no reports of attacks on individuals for their online activities during the coverage period, online journalists were frequently targeted for harassment and intimidation in 2013 and early 2014. Between June and September 2013, the government targeted individuals suspected of writing anonymously for the critical online news outlets, Zambian Watchdog and Zambia Reports, including

---


⁵⁹ Zambian Watchdog, Facebook Post, September 2, 2013, [http://on.fb.me/1PkfujQ](http://on.fb.me/1PkfujQ).


⁶⁵ Electronic Communications and Transaction Act No. 21 of 2009, Part IX, Domain Name Regulation.

⁶⁶ Electronic Communications and Transaction Act No. 21 of 2009, Part IX, Domain Name Regulation, art. 52.
Zambia

Thomas Zyumbo, Clayson Hamasaka, and Wilson Pondamali who were all harassed and subsequently arrested. Zyumbo was reportedly threatened and physically assaulted by President Sata’s son for unknown reasons in March 2014. Pondamali was attacked in April 2014 at a public event, allegedly by government “thugs” who took off with his digital equipment.

Technical Attacks

Government-sponsored technical attacks against opposition activists, ordinary users, or online journalists are not common in Zambia and were not reported during the coverage period. The last reported technical attack occurred in April 2014 when the website of the Media Institute for Southern Africa (MISA) was hacked alongside a number of government websites by hackers from the Middle East. Zambian Watchdog was last attacked with a DDoS attach in May 2012 that brought the site down for about eight hours.

Zimbabwe

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>55</td>
<td>56</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Key Developments: June 2014 – May 2015

- Frequent power outages disrupted ICT networks, resulting in cutoffs of both mobile networks and internet connections for hours at a time (see Availability and Ease of Access).

- The Facebook page of the anonymous whistleblower “Baba Jukwa” was deleted in July 2014, though the manner in which it was taken down remains shrouded in mystery (see Content Removal).

- In July 2014, criminal defamation was declared unconstitutional under the old constitution but left valid under the new 2013 constitution (see Legal Environment).

- Police arrested and charged two individuals with plotting to overthrow the government for their alleged association with Baba Jukwa (see Prosecutions and Detentions for Online Activities).

- The leader of the “Occupy Africa Unity Square” movement initiated on Facebook was abducted in March 2015 and remained missing as of June 2015 (see Intimidation and Violence).

Population: 14.7 million

Internet Penetration 2014: 20 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: No

Bloggers/ICT Users Arrested: Yes

Press Freedom 2015 Status: Not Free
Zimbabwe

Introduction

Zimbabwe's socioeconomic and political challenges deepened this past year, owing to continued infighting over who will succeed President Robert Mugabe when he decides to step down. In response to the growing instability, the ruling party Zimbabwe African National Union—Patriotic Front (ZANU-PF) took steps to crack down on criticism in general, and frequently targeted communications disseminated via information and communications technologies (ICTs) in particular. Most notably, the government succeeded in taking down the popular Facebook page of the anonymous whistleblower, “Baba Jukwa,” and arrested two individuals suspected of administering the page in July 2014. A university student was also arrested for a Facebook post on the Baba Jukwa page that allegedly undermined state security. Online journalists and ordinary users also faced more harassment, threats, and violence for criticizing the ruling party, especially President Mugabe, this past year. The opposition party, Zimbabwe African People's Union—Federal Party (ZAPU-FP), reported experiencing a cyberattack in early 2015, in advance of various party congresses.

Obstacles to Access

New taxes on ICT gadgets and mobile airtime levied in 2014 made costs of access more expensive, disproportionately impacting the poor. Prolonged power blackouts disrupted ICT networks, resulting in cutoffs of both mobile networks and internet connections for hours at a time. The independence of the regulator POTRAZ was called into question following the cancellation of Telecel's license over a politically charged shareholding dispute.

Availability and Ease of Access

Zimbabwe's internet access is expanding incrementally, growing from a penetration rate of 19 percent in 2013 to 20 percent in 2014, according to estimates by the International Telecommunication Union (ITU). By contrast, official government statistics report an internet penetration rate of 50 percent as of December 2014, up from 42 percent in 2013, which includes both fixed-line and mobile internet subscriptions. Approximately 99 percent of internet access is via mobile telephony, while access via fixed-line internet remains low at less than 1 percent. The mobile phone penetration rate, which is over 100 percent, includes users with multiple SIM cards, thus belying the actual number of Zimbabweans who have access to mobile services—estimated at only 60 percent.

Increasing investments in the country's telecommunications infrastructure in recent years have made service prices more affordable for consumers. In 2014, the leading internet service provider (ISP), Liquid, launched its Fiber-to-Home (FTH) service after laying fiber-optic cables in nearly all major towns and now offers a start-up price for homes of US$39 per month for up to 15GB per month. State-owned ISP TelOne also worked to extend ADSL broadband services across the country throughout 2014, reaching almost all small towns to provide broadband to its clients through a

---

5 For 5Mbps download and up to 1Mbps upload.
prepaid service of 10GB for US$25.\(^6\) Despite improvements, effective broadband for home and individual users has not been fully realized due to poor infrastructure and a lack of reliable electricity. In 2014, fixed-broadband subscriptions remained low at a penetration rate of merely 1 percent.\(^7\)

While Zimbabweans have benefitted from low-cost, internet-enabled imitation mobile phones imported from Asia, new taxes on ICTs levied in 2014 increased the cost of access, which disproportionately impacted the poor. In September 2014, Finance Mister Patrick Chinamasa introduced a 25 percent import tax on all ICT gadgets on top of an already existing 15 percent value-added tax (VAT) to increase state revenues.\(^8\) He also implemented a 5 percent excise tax on mobile airtime.\(^9\) To help offset the new price increases, the regulator in January 2015 forced mobile phone companies to reduce the cost of voice calls from a peak period charge of 23 cents per minute to 15 cents, and those for SMS from 9-10 cents to 5 cents.\(^10\)

While most Zimbabweans access the internet via mobile phones, cybercafes are still playing a key role as internet access points. A combination of web surfing, gaming, and music and video downloads is attracting mostly urban youth back to internet cafes, which are increasingly found in nearly every rural district center.\(^11\) Nonetheless, there remains a significant urban-rural divide in access to both internet and mobile technologies, particularly as a result of major infrastructural limitations in rural areas, such as poor roads and electricity distribution. Even in urban areas, electricity is regularly rationed for six to seven hours a day, leading to uneven access to internet and mobile phone services. In 2014-2015, frequent power outages affected both households and business entities such as cybercafes, resulting in cutoffs of both mobile networks and internet connections for hours at a time.

**Restrictions on Connectivity**

No cases of deliberate disruptions in connectivity were recorded during the coverage period, compared to the previous period, when the independent community radio station, Radio Dialogue, reported frequent internet disconnections in its office in the lead-up to the July 2013 general elections, and internet cafe owners reported slow internet connectivity.\(^12\) While the government’s hand in the disruptions could not be confirmed, state control over two of the country’s five international gateways, as well as the state’s ability to issue directives to private telecom providers, increase the likelihood of deliberate government interference.

Two of Zimbabwe’s five international gateways for internet and voice traffic are operated by the state-owned fixed network, TelOne, and mobile network, NetOne. The private mobile operators—Econet, TeleCel, and Africom—operate the other three international gateways.\(^13\) In mid-2014, government officials expressed discontent with the country’s “sporadic international gateways” and stat-

---


\(^11\) From research via calls to relatives and friends who live near rural business centers as well as personal visits to some rural centers.


Zimbabwe

...ed intentions to intervene with a national policy, leading to concerns that the government is trying to increase its control over the operations of Zimbabwe’s internet gateways.

ICT Market

Zimbabwe currently has 28 ISPs, representing a competitive market for internet service provision. As set by the regulator, the license fees for ISPs range from US$2-4 million, depending on the type of service to be provided, and must be vetted and approved by the regulator prior to installation. Providers must also pay 3.5 percent of their annual gross income to the regulator. By contrast, mobile services are provided by three operators, two of which are privately owned—Econet Wireless and Telecel. The government has complete ownership of the third operator, NetOne, but is reportedly seeking to privatize up to 60 percent of company.

Regulatory Bodies

ISPs and mobile phone companies are regulated by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), whose leaders are appointed by the president in consultation with the minister of transport and communication. While POTRAZ handles the official licensing process for telecoms, insider reports have revealed a growing interest of the military intelligence in the operations of telecoms companies. The military intelligence and the Central Intelligence Organization are known to screen and approve license applications, demonstrating how the state regards ICTs as a security matter.

POTRAZ has been widely accused of partisanship and politicized decision-making, as evidenced in early 2015 when the regulator revoked of the license of the country’s third largest mobile phone operator, Telecel. At the time, Telecel was embroiled in a shareholding dispute that pit President Mugabe’s nephews Patrick Zhuwao and Leo Mugabe against other shareholders. The intervention was seen as part of a political move to protect and advance the interests of those close to the Mugabe family. On May 7, 2015, the High Court ordered POTRAZ to reinstate the Telecel license.

Limits on Content

Civil society organizations reported having trouble disseminating bulk SMS text messages throughout 2014 and 2015, particularly messages perceived as political by the state. In response, organized civic activism is finding space through WhatsApp groups made up of citizen journalists and ordinary users.

Zimbabwe

The Facebook page of the anonymous whistleblower “Baba Jukwa” was deleted in July 2014, though the manner in which it was taken down remains unclear.

Blocking and Filtering

No websites were blocked or filtered in Zimbabwe during the coverage period. Access to social media platforms such as Facebook, Twitter, and YouTube and international blog-hosting platforms are all freely available, though the government regards Facebook and other communications platforms as sources of political subversion and has indicated intentions to block the websites over the past few years.21

By contrast, civil society organizations reported having trouble disseminating bulk SMS text messages throughout 2014 and 2015, particularly messages perceived as political by the state. A ban on bulk SMS services was originally implemented in the lead-up to the 2013 elections.22 The ban, which was not made known to the public, effectively obstructed the ability of civil society groups to send SMS messages with election-related information, and there were no mechanisms in place for appeal.23 Meanwhile, ZANU-PF members routinely sent bulk SMS messages via all networks on behalf of President Robert Mugabe’s campaign and other ruling party candidates.

Content Removal

Zimbabwean government authorities and opposition leaders frequently pressured users and content producers to delete content from social media platforms during the coverage period, reflecting a growing trend compared to previous years.

Most notably, the Facebook page of the anonymous whistleblower Baba Jukwa was deleted in July 2014, though the manner in which it was removed remains shrouded in mystery. Most accuse the Zimbabwean government, which had reportedly sent senior police officials to the United States in late 2014 to liaise directly with Facebook and convince the company to delete the page, which was followed by nearly half a million users.24 The president had also reportedly sought Chinese technical assistance in censoring the page and identifying its owner in previous years.25 Some believe the authorities had managed to hack into and take control of the Baba Jukwa page to delete the profile. Either way, the page was ultimately taken down in July 2014,26 after an editor at the Sunday Mail state newspaper, Edmund Kudzayi, was arrested in June on accusations of running the Baba Jukwa account (see “Prosecutions and Detentions for Online Activities”).27

23 One such ICT based Civic network Kubatana.net issued a statement stating that, “…in the run-up to Zimbabwe’s 2013 election, our ability to send bulk text messages has been blocked. We have been informed by Econet that their regulator, Potraz, has issued a directive blocking the delivery of bulk messages from international gateways. “Potraz Bans Bulk SMSs,” News Day, July 26, 2013, http://bit.ly/1Ga9G3k.
Zimbabwe

Social networking pages and chat groups were also targeted for removal by opposition leader Morgan Tsvangirai, who in May 2015 ordered all WhatsApp and Facebook groups administered by any members of the Movement for Democratic Change (MDC) opposition party to shut down or face suspension. Tsvangirai, who heads the MDC, was allegedly irked by public debates held on social media platforms between the party’s senior officials. Following the ban, the party reportedly suspended five of its officials based in the city of Bulawayo on May 10, 2015 for “allegedly abusing social media platforms to attack the party’s top leadership.”

A mobile money account belonging to the ZAPU-FP opposition party was shut down in early 2015, which some observers believe was politically motivated. Created for fundraising purposes, ZAPU-FP’s account with Econet’s mobile money service Ecocash was shut down with no explanation from the provider, leading ZAPU-FP party members to suspect Econet of acting on instructions from the security sector.

Media, Diversity, and Content Manipulation

Media surveys indicate a continuing decline in newspaper readership coinciding with the rising use of ICT-based platforms for news and other information. This trend has prompted newspapers to work on integrating online platforms. The popular Mobi News service for mobile devices launched by Alpha Media Holdings—the group publisher of *The Standard, Newsday, Southern Times,* and *Zimbabwe Independent*—now attracts more subscription revenue than the firm’s print publications.

Independent news websites and other digital media outlets based outside Zimbabwe provide critical sources of information for Zimbabwean citizens, especially on taboo subjects that local media groups are afraid of covering due to fears of government reprisal. These diaspora-based outlets, such as New.zimbabwe.com and Nehanda-radio.com, post reports on sensitive issues by local journalists and citizens who write under pseudonyms, a practice employed by many journalists to avoid harassment. Few independent news outlets are based in the country.

Ordinary citizens are also increasingly using pseudonyms online to discuss political topics, and following the arrest of the suspected owner of the anonymous Baba Jukwa account in July 2014 (see “Prosecutions and Detentions for Online Activities”), users have increasingly opted to self-censor out of concerns over the state’s capacity to seek out the identities of pseudonymous individuals. Suspicions of pervasive state surveillance have also led to increasing self-censorship, particularly on issues that involve the military, the intelligence, President Robert Mugabe, and the first family.

---

Zimbabwe

Digital Activism

Despite fears of being identified, organized civic activism is finding space through WhatsApp groups made up of citizen journalists and ordinary users sharing community information and seeking to influence local government decisions. Social media is increasingly used to engage with local authorities on service delivery and to mobilize communities around various issues. Nevertheless, various mobilization efforts have yet to manifest in any meaningful social, political, or economic change in Zimbabwe.

In late 2014, the Facebook group “Occupy Africa Unity Square” was launched, demanding President Mugabe admit failure and step down from power. The group, which has garnered hundreds of thousands of followers, organized a series of peaceful protests in October and November, which were met with heavy-handed resistance by riot police who used violence to disburse the protests. The leader of the “Occupy Africa Unity Square” movement was later abducted for his activism in March 2015; he remained missing as of June 2015 (see “Intimidation and Violence”).

Violations of User Rights

The Zimbabwean Constitutional Court declared criminal defamation unconstitutional under the old constitution but left it valid under the new 2013 constitution. Numerous individuals were targeted for their alleged association with Baba Jukwa, leading to several arrests. Online journalists and ordinary users faced more harassment, threats, and violence for criticizing the government online in the past year. The opposition party, ZAPU-FP, reported experiencing a hacking attack in early 2015, in advance of various party congresses.

Legal Environment

The 2013 Zimbabwe constitution outlines rights for media, free expression, and access to information and broadcasting for citizens, though numerous other pieces of legislation violate these constitutional rights. Chief among such laws is the Access to Information and Protection of Privacy Act (AIPPA), under which all journalists are accredited and media houses registered. Among its limiting provisions, the AIPPA provides for a Media Commission that has powers to ban journalists and media organizations and places restrictions on reporting on a broad range of government information. Bloggers, however, are not eligible for accreditation as journalists under the AIPPA.

Restrictions on certain types of speech under the Criminal Law Codification and Reform Act (CODE) remain on the books and apply equally to reporters in traditional media and online. The CODE criminalizes defamation, punishing anyone who publicly undermines the authority of the president or insults him in any printed or electronic medium with a sentence of up to 20 years in prison. In an apparent sleight of hand, the Zimbabwean Constitutional Court struck down criminal defamation

Zimbabwe

under the CODE in July 2014, declaring it unconstitutional under the old constitution, but left it valid under the new 2013 constitution.

In April 2015, the government announced plans to draft the Cyber Crime and Data Protection Bill, which purportedly aims to curb criminal activities. Given the state's tendency to include civic and political activism as part of its broad definition of what is considered "criminal," human rights defenders fear the law will be abused to crack down on social media activities.

The state's legal restrictions are sometimes balanced by the judiciary, which has demonstrated a degree of autonomy through several rulings that have not been favorable to the state, including some freedom of expression cases. Nevertheless, an appointment process that allows for high levels of executive interference compromises judicial independence.

Prosecutions and Detentions for Online Activities

In 2014, the Zimbabwean authorities ramped up their efforts to silence the anonymous Baba Jukwa whistleblower, whose Facebook page posted frequent allegations of corruption against ruling party members and had nearly a half a million followers before it was shut down in July 2014 (see “Content Removal”). Numerous individuals were targeted for their alleged association with Baba Jukwa, including South Africa-based journalist Mxolisi Ncube, who was questioned by police at the Zimbabwean embassy in Pretoria, South Africa in June 2014 for his suspected connection to the Facebook profile. Police also questioned senior government ministers—including Information Minister Jonathan Moyo, Environment Minister Savior Kasukuwere, and former ruling party spokesperson Rugare Gumbo—over the Baba Jukwa case.

On June 19, 2014, the authorities arrested the former editor of the state-owned The Sunday Mail newspaper, Edmund Kudzayi, on accusations of running the Baba Jukwa Facebook page. Five days later, police also arrested Kudzayi’s brother Phillip on allegations of being a co-administrator and charged both with plotting to overthrow the government. The government’s crackdown on Baba Jukwa continued with the arrest of University of Zimbabwe student Romeo Musemburi in late June 2014 for a Facebook post on the Baba Jukwa page that allegedly undermined state security. Charges against the Kudzayi brothers were eventually withdrawn in May 2015 for lack of evidence, as well as those against Musemburi in June 2015.
Meanwhile, the long running case against Shantel Rusike, who was arrested on December 24, 2012 and accused of distributing a nude picture of President Mugabe on WhatsApp, was finally heard by the Constitutional Court in January 2015. Rusike faces charges of “causing hatred, contempt or ridicule of the president,” as delineated in the CODE. Court justices indicated that the case may be dismissed, with one justice stating that a WhatsApp message does not constitute public dissemination. The Constitutional Court’s judgment had not been released as of mid-2015.

Surveillance, Privacy, and Anonymity

There were numerous reports of surveillance abuse during the coverage period, beginning with the arrest of Phillip Kudzayi in July 2014 on suspicions of his connection to the Baba Jukwa Facebook whistleblower. Police claimed they tracked communications linked to Baba Jukwa to a mobile phone line registered under Kudzayi’s name. Meanwhile, state media employees and senior government officials were reportedly under constant surveillance throughout the year, as tensions remained high over post-Mugabe succession politics. Observers believe surveillance has allowed President Mugabe to expel several disloyal government officials who he accused of plotting his downfall.

Such surveillance abuse is enabled by the government’s ability to monitor and intercept user data and communications without adequate oversight. Several laws provide the authorities with a legal mechanism to conduct surveillance of citizens’ activities online, including the Post and Telecommunications Act of 2000, which allows the government to intercept suspicious communications and requires a telecommunications licensee, such as an ISP, to supply information to government officials upon request. The act also obligates telecoms to report any communications with “offensive” or “threatening” content.

Under the Interception of Communications Act of 2007, the Monitoring of Interception of Communications Center has the power to oversee traffic in all telecommunications services and to intercept phone calls, emails, and faxes under the pretext of national security. The Act further requires telecommunications operators and ISPs to install necessary surveillance technology at their own expense and to intercept information on the state’s behalf. Failure to comply is punishable with a fine and sentence of up to three years in prison. Warrants allowing the monitoring and interception of communications are issued by the minister of information at his discretion; consequently, there is no adequate judicial oversight or other independent safeguard against abuse, and the extent and frequency of monitoring remains unknown.

Anonymous communication and the privacy of user data are compromised by SIM card registration regulations implemented in 2011, which require mobile phone users to submit personal identity details to mobile operators, ostensibly to combat crime and curtail threatening or obscene communications. Encrypted communication applications such as Skype are accessible, though since

---

49 Section 33(2) (a) (ii) of the Criminal Law (Codification and Reform) Act/CODE Chapter 9:23.
50 Section 33(2) (a) (ii) of the Criminal Law (Codification and Reform) Act/CODE Chapter 9:23.
51 Postal and Telecommunications Act 2000, Part XII, Section 98, “Interception of communications.”
September 2011, POTRAZ has maintained a ban—reportedly for security reasons—on the use of the BlackBerry messenger service that enables users to send free encrypted messages.\(^{56}\)

The scope of subscriber registration requirements expanded under the 2013 Postal and Telecommunications (Subscriber Registration) Regulations (Statutory Instrument 142/2013) to include subscriptions with any “…telecommunication licensees or designated agents who provides telecommunication services,” including internet subscriptions.\(^{57}\) Registration details require a full name, permanent residential address, nationality, gender, subscriber ID number, and national ID or passport number to be submitted to network operators, who are then required to retain such personal information for five years \textit{after} either the subscriber or operator has discontinued service. In addition, the regulations require ISPs to provide POTRAZ with copies of their subscriber records to be stored in a Central Subscriber Information Database to enable POTRAZ to “assist law enforcement agencies on safeguarding national security,” among other aims.\(^{58}\) Officials could petition POTRAZ for access to the subscriber database without a court order.

In a positive step in June 2014, the government repealed the legal provision in the 2013 Subscriber Registration Regulations that allowed security agents to access user information from a central database without a court-issued warrant, after the Parliamentary Legal Committee (PLC) found provisions of the new regulations unconstitutional.\(^{59}\) An amended version of the regulations—the Statutory Instrument 95/2014—was subsequently enacted in July 2014, which requires law enforcement agents to obtain a court order to request information from the central database.\(^{60}\) Analysis by the Zimbabwean legal watchdog Veritas, however, found this amendment to fall short of judicial oversight, since it requires either a court order or a warrant, the latter of which “can be issued by police officers who have been designated as justices of the peace.”\(^{61}\)

Intimidation and Violence

Online journalists and ordinary users faced more harassment, threats, and violence for criticizing the ruling party, especially President Mugabe, online in the past year. Incidents during the coverage period included:

- University of Zimbabwe student Romeo Musemburi, who was arrested in June 2014 for a Facebook post on the Baba Jukwa page, reported being beaten while in police custody.
- In late 2014, residents of Mbare, a high-density neighborhood in the capital Harare, were...

\(^{56}\) The ban went into effect in response to unfounded fears that the service had facilitated the 2011 Arab uprisings as well as the violent protests that took place in England in August of the same year. In mid-2011, POTRAZ director general Charles Manzi Sibanda announced that the regulator was examining the compliance of BlackBerry’s encryption technology with the Interception of Communications Act, which requires that all telecommunication services allow official interception. The POTRAZ decision was still outstanding as of December 2013. BlackBerry formerly operated as Research in Motion. See, “BlackBerry Messenger a dream,” \textit{The Zimbabwean}, June 5, 2012, \url{http://bit.ly/1Pxsz2i}.


\(^{58}\) Postal and Telecommunications (Subscriber Registration) Regulations, 2013, Section 8 (1) and (2).


\(^{60}\) Postal and Telecommunications (Subscriber Registration) Regulations, 2014, \url{http://www.cfuzim.org/images/si9514.pdf}.

reportedly harassed by ZANU-PF youths who forcibly searched the residents’ WhatsApp messages for anti-Mugabe texts.

- In February 2015, photojournalists were forced to delete photos and videos from their devices that had captured Mugabe falling to the ground at the airport.  

- In March 2015, political activist Itai Dzamara was abducted near his Harare home, spawning an online wave of protests calling for his return and decrying the government’s inaction on the matter. Dzamara was known for his leadership of the “Occupy Africa Unity Square” protest group organized on Facebook and had received numerous threats from state security agents for his activism prior to his disappearance. He remained missing as of mid-2015.

### Technical Attacks

Technical attacks against critical websites and social media pages have increased in recent years. The Facebook page of anonymous whistleblower Baba Jukwa reportedly faced frequent hacking attempts to take the page down throughout 2014, which may have succeeded in removing the page altogether in July 2014 (see "Content Removal"). The opposition party, ZAPU-FP, also reported experiencing a cyberattack in early 2015. Its timing in advance of the party’s preparations for its youth and women congresses in April 2015 and the main congress in August led party members to suspect the hack was politically motivated.

---

63 “61 Days: Police doing nothing about Dzamara.”
64 See Occupy Africa Unity Square, Facebook Page, [http://on.fb.me/1OznoLe](http://on.fb.me/1OznoLe).
65 See Bring Back Itai Dzamara Now, Facebook Page, [http://on.fb.me/1Lpom503](http://on.fb.me/1Lpom503).
Methodology

*Freedom on the Net* provides analytical reports and numerical scores for 65 countries worldwide. Assigning scores allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. The country reports provide narrative detail to support the scores. *Freedom on the Net* also documents censorship methods used by different countries in an annual chart (see “Key Internet Controls By Country”).

The countries were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom. The ratings and reports included in this study particularly focus on developments that took place between June 1, 2014 and May 31, 2015.

*Freedom on the Net* is a collaborative effort between a small team of Freedom House staff and an extensive network of local researchers and advisors in 65 countries. Our in-country researchers have diverse backgrounds—academia, blogging, traditional journalism, and tech—and track developments from their country of expertise. In the most repressive environments, Freedom House takes care to ensure researchers’ anonymity or, in exceptional cases, works with individuals living outside their home country.

**What We Measure**

The *Freedom on the Net* index measures each country’s level of internet and digital media freedom based on a set of methodology questions developed in consultation with international experts to capture the vast array of relevant issues that enable internet freedom (see “Checklist of Questions”). Given increasing technological convergence, the index also measures access and openness of other digital means of transmitting information, particularly mobile phones and text messaging services.

Freedom House does not maintain a culture-bound view of freedom. The project methodology is grounded in basic standards of free expression, derived in large measure from Article 19 of the Universal Declaration of Human Rights:

> “Everyone has the right to freedom of opinion and expression; this right includes freedom

to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers.”

This standard applies to all countries and territories, irrespective of geographical location, ethnic or religious composition, or level of economic development.

The project particularly focuses on the transmission and exchange of news and other politically relevant communications, as well as the protection of users’ rights to privacy and freedom from both legal and extralegal repercussions arising from their online activities. At the same time, the index acknowledges that in some instances freedom of expression and access to information may be legitimately restricted. The standard for such restrictions applied in this index is that they be implemented only in narrowly defined circumstances and in line with international human rights standards, the rule of law, and the principles of necessity and proportionality. As much as possible, censorship and surveillance policies and procedures should be transparent and include avenues for appeal available to those affected.

The index does not rate governments or government performance per se, but rather the real-world rights and freedoms enjoyed by individuals within each country. While digital media freedom may be primarily affected by state actions, pressures and attacks by nonstate actors, including the criminal underworld, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental, including private corporations.

**The Scoring Process**

The methodology includes 21 questions and nearly 100 subquestions, divided into three categories:

- **Obstacles to Access** details infrastructural and economic barriers to access, legal and ownership control over internet service providers, and independence of regulatory bodies;
- **Limits on Content** analyzes legal regulations on content, technical filtering and blocking of websites, self-censorship, the vibrancy and diversity of online news media, and the use of digital tools for civic mobilization;
- **Violations of User Rights** tackles surveillance, privacy, and repercussions for online speech and activities, such as imprisonment, extralegal harassment, or cyberattacks.

Each question is scored on a varying range of points. The subquestions guide researchers regarding factors they should consider while evaluating and assigning points, though not all apply to every country. Under each question, a lower number of points is allotted for a more free situation, while a higher number of points is allotted for a less free environment. Points add up to produce a score for each of the subcategories, and a country’s total points for all three represent its final score (0-100). Based on the score, Freedom House assigns the following internet freedom ratings:

- Scores 0-30 = Free
- Scores 31-60 = Partly Free
- Scores 61-100 = Not Free

After researchers submitted their draft scores in 2015, Freedom House convened five regional review meetings and numerous international conference calls, attended by Freedom House staff and over 70 local experts, scholars, and civil society representatives from the countries under study. During the meetings, participants reviewed, critiqued, and adjusted the draft scores—based on set coding guidelines—through careful consideration of events, laws, and practices relevant to each item. After completing the regional and country consultations, Freedom House staff did a final review of all scores to ensure their comparative reliability and integrity.

**Key Internet Controls Explained**

In the Key Internet Controls table (page 16-17), Freedom House staff document the prevalence of different censorship methods by marking incidents of their occurrence in each country. Incidents are based on Freedom on the Net research and verified by in-country researchers. Inclusion in the table indicates the internet control occurred at least once during the coverage period of the report, unless otherwise indicated.

1. **Social media or communications apps blocked:** Entire platforms temporarily or permanently blocked to prevent communication and information sharing.

2. **Political, social, or religious content blocked:** Blocking or filtering of domains, URLs, or keywords, to limit access to specific content.

3. **Localized or nationwide ICT shut down:** Intentional disruption of internet or cellphone networks in response to political or social events, whether temporary or long term.

4. **Progovernment commentators manipulate online discussions:** Strong indications that individuals are paid to distort the digital information landscape in the government’s favor, without acknowledging sponsorship.

5. **New law or directive increasing censorship or punishment passed:** Any legislation adopted or amended during the coverage period, or any directive issued, to censor or punish legitimate online activity.

6. **New law or directive increasing surveillance or restricting anonymity passed:** Any legislation adopted or amended during the coverage period, or any directive issued, to surveil or expose the identity of citizens using the internet with legitimate intent.

7. **Blogger or ICT user arrested, imprisoned, or in prolonged detention for political or social content:** Any arrest or detention that is credibly perceived to be in reprisal for digital expression, including trumped up charges. Brief detentions for interrogation are not reflected.

8. **Blogger or ICT user physically attacked or killed (including in custody):** Any physical attack that is credibly perceived to be in reprisal for digital expression, including kidnapping and torture.

9. **Technical attacks against government critics and human rights organizations:** Cyberattacks against individuals sharing information perceived as critical, with the clear intent of disabling content or exposing user data, and motives that align with those of agencies that censor and surveil the internet. Targets may include critics in exile, but not transnational cyberattacks, even with political motives.
Checklist of Questions

- Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- A combined score of 0-30=Free, 31-60=Partly Free, 61-100=Not Free.

**A. OBSTACLES TO ACCESS (0-25 POINTS)**

1. To what extent do infrastructural limitations restrict access to the internet and other ICTs? (0-6 points)
   - Does poor infrastructure (electricity, telecommunications, etc.) limit citizens’ ability to receive internet in their homes and businesses?
   - To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?
   - To what extent is there internet and mobile phone access, including data connections or satellite?
   - Is there a significant difference between internet and mobile phone penetration and access in rural versus urban areas or across other geographical divisions?
   - To what extent are broadband services widely available in addition to dial-up?

2. Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)
   - In countries where the state sets the price of internet access, is it prohibitively high?
   - Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?
   - Do low literacy rates (linguistic and “digital literacy”) limit citizens’ ability to use the internet?
   - Is there a significant difference between internet penetration and access across ethnic or socioeconomic societal divisions?
   - To what extent are online software, news, and other information available in the main local languages spoken in the country?

3. Does the government impose restrictions on ICT connectivity and access to particular social media and communication apps permanently or during specific events? (0-6 points)

4. Are there legal, regulatory, or economic obstacles that prevent the existence of diverse business entities providing access to digital technologies? (0-6 points)
   - Note: Each of the following access providers are scored separately:
   1a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)
   1b. Cybercafes and other businesses entities that allow public internet access (0-2 points)
   1c. Mobile phone companies (0-2 points)
   - Is there a legal or de facto monopoly over access providers or do users have a choice of access provider, including ones privately owned?
   - Is it legally possible to establish a private access provider or does the state place extensive legal or regulatory controls over the establishment of providers?
   - Are registration requirements (i.e. bureaucratic “red tape”) for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?
   - Does the state place prohibitively high fees on the establishment and operation of access providers?
5. To what extent do national regulatory bodies overseeing digital technology operate in a free, fair, and independent manner? (0-4 points)
- Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?
- Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders’ interests?
- Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?
- Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?
- Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?

B. LIMITS ON CONTENT (0-35 POINTS)

1. To what extent does the state or other actors block or filter internet and other ICT content, particularly on political and social issues? (0-6 points)
- Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?
- Is there significant filtering of text messages or other content transmitted via mobile phones?
- Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of email or text messages, etc?
- Are methods such as deep-packet inspection used for the purposes of preventing users from accessing certain content or for altering the content of communications en route to the recipient, particularly with regards to political and social topics?

2. To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? (0-4 points)
- To what extent are non-technical measures—judicial or extra-legal—used to order the deletion of content from the internet, either prior to or after its publication?
- To what degree do government officials or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?
- Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?
- Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?

3. To what extent are restrictions on internet and ICT content transparent, proportional to the stated aims, and accompanied by an independent appeals process? (0-4 points)
- Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?
- Are state authorities transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?
- Do state authorities block more types of content than they publicly declare?
- Do independent avenues of appeal exist for those who find content they produced to have been subjected to censorship?

4. Do online journalists, commentators, and ordinary users practice self-censorship? (0-4 points)
- Is there widespread self-censorship by online journalists, commentators, and ordinary users in state-run online media, privately run websites, or social media applications?
- Are there unspoken "rules" that prevent an online journalist or user from expressing certain opinions in ICT communication?
- Is there avoidance of subjects that can clearly lead to harm to the author or result in almost certain censorship?

5. To what extent is the content of online sources of information determined or manipulated by the government or a particular partisan interest? (0-4 points)
- To what degree do government officials or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?
- Do authorities issue official guidelines or direc-
tives on coverage to online media outlets, blogs, etc., including instructions to marginalize or amplify certain comments or topics for discussion?

- Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?
- Does the government employ, or encourage content providers to employ, individuals to post pro-government remarks in online bulletin boards and chat rooms?
- Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?

6. Are there economic constraints that negatively impact users’ ability to publish content online or online media outlets’ ability to remain financially sustainable? (0-3 points)

- Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, email applications, blog hosting platforms, etc.) to be economically viable?
- Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?
- Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?
- To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect “net neutrality” with regard to content)?
- To what extent do users have access to free or low-cost blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?

7. To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content? (0-4 points)

- Are people able to access a range of local and international news sources via the internet or text messages, despite efforts to restrict the flow of information?
- Does the public have ready access to media outlets or websites that express independent, balanced views?
- Does the public have ready access to sources of information that represent a range of political and social viewpoints?
- To what extent do online media outlets and blogs represent diverse interests within society, for example through websites run by community organizations or religious, ethnic and other minorities?
- To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?

8. To what extent have individuals successfully used the internet and other ICTs as sources of information and tools for mobilization, particularly regarding political and social issues? To what extent are such mobilization tools available without government restriction? (0-6 points)

- To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or the behavior of other powerful societal actors?
- To what extent are online communication tools or social networking sites (e.g. Twitter, Facebook) used as a means to organize politically, including for “real-life” activities?
- Are mobile phones and other ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?

C. VIOLATIONS OF USER RIGHTS (0-40 POINTS)

1. To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)

- Does the constitution contain language that provides for freedom of speech and of the press generally?
- Are there laws or legal decisions that specifically protect online modes of expression?
- Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?
- Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?
- Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?
2. Are there laws which call for criminal penalties or civil liability for online and ICT activities? (0-4 points)
   - Are there specific laws criminalizing online expression and activity such as posting or downloading information, sending an email, or text message, etc.? (Note: this excludes legislation addressing harmful content such as child pornography or activities such as malicious hacking)
   - Do laws restrict the type of material that can be communicated in online expression or via text messages, such as communications about ethnic or religious issues, national security, or other sensitive topics?
   - Are restrictions of internet freedom closely defined, narrowly circumscribed, and proportional to the legitimate aim?
   - Are vaguely worded penal codes or security laws applied to internet-related or ICT activities?
   - Are there penalties for libeling officials or the state in online content?
   - Can an online outlet based in another country be sued if its content can be accessed from within the country (i.e. "libel tourism")?

3. Are individuals detained, prosecuted or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs, particularly on political and social issues? (0-6 points)
   - Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?
   - Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via email or text messages?
   - Does the lack of an independent judiciary or other limitations on adherence to the rule of law hinder fair proceedings in ICT-related cases?
   - Are individuals subject to abduction or arbitrary detention as a result of online activities, including membership in certain online communities?
   - Are penalties for “irresponsible journalism” or “rumor mongering” applied widely?
   - Are online journalists, bloggers, or others regularly prosecuted, jailed, or fined for libel or defamation (including in cases of “libel tourism”)?

4. Does the government place restrictions on anonymous communication or require user registration? (0-4 points)
   - Are website owners, bloggers, or users in general required to register with the government?
   - Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names or register with the government?
   - Are users prohibited from using encryption software to protect their communications?
   - Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?

5. To what extent is there state surveillance of internet and ICT activities without judicial or other independent oversight, including systematic retention of user traffic data? (0-6 points)
   - Do the authorities regularly monitor websites, blogs, and chat rooms, or the content of email and mobile text messages?
   - To what extent are restrictions on the privacy of digital media users transparent, proportional to the stated aims, and accompanied by an independent process for lodging complaints of violations?
   - Where the judiciary is independent, are there procedures in place for judicial oversight of surveillance and to what extent are these followed?
   - Where the judiciary lacks independence, is there another independent oversight body in place to guard against abusive use of surveillance technology and to what extent is it able to carry out its responsibilities free of government interference?
   - Is content intercepted during internet surveillance admissible in court or has it been used to convict users in cases involving free speech?

6. To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users? (0-6 points)
   Note: Each of the following access providers are scored separately:
   6a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)
   6b. Cybercafes and other business entities that allow public internet access (0-2 points)
   6c. Mobile phone companies (0-2 points)
   - Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?
   - Are access providers prosecuted for not doing so?
   - Does the state attempt to control access provid-
ers through less formal methods, such as codes of conduct?
• Can the government obtain information about users without a legal process?

7. Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor? (0–5 points)
  • Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?
  • Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?
  • Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?
  • Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?

8. Are websites, governmental and private entities, ICT users, or service providers subject to widespread “technical violence,” including cyberattacks, hacking, and other malicious threats? (0–3 points)
  • Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks (e.g. cyberespionage, data gathering, DDoS attacks), including those originating from outside of the country?
  • Have websites belonging to opposition or civil society groups within the country’s boundaries been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?
  • Are websites or blogs subject to targeted technical attacks as retribution for posting certain content (e.g. on political and social topics)?
  • Are laws and policies in place to prevent and protect against cyberattacks (including the launching of systematic attacks by nonstate actors from within the country’s borders) and are they enforced?
Contributors

Freedom House Research Team
- Sanja Kelly, Project Director, Freedom on the Net
- Mai Truong, Senior Program Officer (Africa)
- Madeline Earp, Research Analyst (Asia)
- Laura Reed, Research Analyst (Eurasia, EU & Western countries)
- Adrian Shahbaz, Research Analyst (MENA & EU)
- Alexandra Ellerbeck, Senior Research Assistant (Latin America)

Report Authors and Advisors
- Argentina: Eduardo Andres Bertoni, Director, Center for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law, Argentina; Daniela Schnidrig, Researcher, CELE
- Armenia: Seda Muradyan, Armenia Country Director, Institute for War and Peace Reporting; Samvel Martirosyan, Head of Board, Institute for Strategic and Innovative Research
- Australia: Dr. Alana Maurushat, Senior Lecturer, Faculty of Law, and Co-Director, Cyberspace Law and Policy Community, The University of New South Wales
- Azerbaijan: Arzu Geybulla, Azerbaijani journalist and blogger
- Bangladesh: Dr. Faheem Hussain, Assistant Professor, Department of Technology and Society, State University of New York (SUNY) Korea
- Brazil: Fabricio Bertini Pasquot Polido, Professor, Law School of the Federal University of Minas Gerais, and Head of the Center for International Studies on Internet, Innovation, and Intellectual Property (GNET); Carolina Rossini, Vice President of International Policy, Public Knowledge, and Board Member, Open Knowledge Foundation, InternetLab, and CodingRights
- Cambodia: Sopheap Chak, Executive Director, Cambodian Center for Human Rights, and human rights blogger
- Canada: Michael Geist, Canada Research Chair in Internet and E-commerce Law, Faculty of Law, University of Ottawa
- China: Sarah Hoffman, Youth Free Expression Program Manager, National Coalition Against Censorship, and China researcher; Wen Yunchao ("Beifeng"), Chinese blogger and activist
- Colombia: Law, Internet, and Society Group, Fundación Karisma
- Cuba: Ernesto Hernández Busto, Cuban journalist and writer
- Estonia: Linnar Viik, Associate Professor, Estonian IT College
- France: Jean-Loup Richet, Researcher, University of Nantes
- Georgia: Teona Turashvili, Analyst, Institute for Development of Freedom of Information (IDFI)
- Germany: Philipp Otto, Founder and Head, iRights. Lab think tank and iRights.Media publishing house, Editor in Chief, iRights.info, political strategist, advisor to the German government and companies; Henning Lahmann, Policy Analyst, iRights.Lab
- Hungary: Borbála Tóth, independent researcher based in Budapest
- Iceland: Caroline Nellemann, independent consultant, specialist in digital media and civic engagement
- India: Chinmayi Arun, Research Director, Center for Communication Governance at National Law University, Delhi; Sarvjeet Singh, Senior Fellow and Project Manager, Centre for Communication Governance; Parul Sharma, Student, B.A., L.L.B. (Hons.), National Law University; with research assistance from students Nishtha Sinha and Vaibhav Dutt, B.A., L.L.B. (Hons.), National Law University
- Indonesia: Enda Nasution, Co-Founder, Sebangsa.com, and independent blogger
- Iran: Mahmood Enayat, Director, Small Media
- Italy: Giampiero Giacomello, Associate Professor of International Relations, University of Bologna
- Japan: Dr. Leslie M. Tkach-Kawasaki, Associate Professor, University of Tsukuba
- Jordan: Lina Ejeilat, Co-founder and Executive Editor, 7iber
- Kazakhstan: Adilzhan Nurmakov, Senior Lecturer, KIMEP University
- Kenya: Grace Githaiga, Associate, Kenya ICT Action Network (KICTANet)
- Kyrgyzstan: Artem Goryainov, IT Programs Director, Public Foundation CIIP
• Lebanon: Firas Talhouk, Researcher, Samir Kassir Foundation
• Libya: Maramaisoud Elbadri, Business Developer, Tatweer Research
• Malawi: Gregory Gondwe, Bureau Chief, Times Media Group, Malawi
• Malaysia: K. Kabilan, Managing Editor, BeritaDaily.com, and online media consultant
• Mexico: Jorge Luis Sierra, Knight International Journalism Fellow, International Center for Journalists, and award-winning Mexican journalist
• Morocco: Bouziane Zaid, Assistant Professor of Media and Communication, Al Akhawayn University in Ifrane
• Myanmar: Min Zin, Burmese journalist, and Contributor, Foreign Policy Democracy Lab
• Nigeria: 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria
• Pakistan: Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan; Muhammad Ismael Khan, Research Associate, Digital Rights Foundation
• Philippines: Jacques D.M. Gimeno, independent researcher based in Manila
• Singapore: Cherian George, Associate Professor, School of Communication, Hong Kong Baptist University
• South Africa: Alex Comninos, independent researcher
• South Korea: Dr. Yenn Lee, Doctoral Training Advisor, School of Oriental and African Studies, University of London
• Sri Lanka: N. V. Nugawela, independent writer and researcher
• Sudan: Azaz Elshami, independent researcher and development consultant
• Syria: Dlshad Othman, Information Security Manager, Information Safety & Capacity Project (ISC)
• Uganda: Lillian Nalwoga, Policy Officer, CIPESA, and President, Internet Society Uganda Chapter
• Ukraine: Tetyana Lokot, Ukrainian journalist; Contributing Editor, RuNet Echo, Global Voices; and Doctoral Candidate, Philip Merrill College of Journalism, University of Maryland
• United Kingdom: LSE Media Policy Project, London School of Economics and Political Science
• United States: Open Technology Institute, New America
• Uzbekistan: Dr. Zhanna Hördegen, Research Associate, University Research Priority Program (URPP) Asia and Europe, University of Zurich, and independent consultant
• Venezuela: Raisa Urribarri, Director, Communications Lab for Teaching, Research and Community Extension (LIESR) at the University of Los Andes
• Zambia: Brenda Bukowa, Lecturer and Researcher, Department of Mass Communication, University of Zambia

The analysts for the reports on Angola, Bahrain, Belarus, Ecuador, Egypt, Ethiopia, The Gambia, Russia, Rwanda, Saudi Arabia, Thailand, Tunisia, Turkey, United Arab Emirates, Vietnam and Zimbabwe are independent internet researchers who have requested to remain anonymous. Freedom on the Net intern Liridona Malota provided invaluable research and administrative assistance in the production of the 2015 edition of the report.
“Digital activism has been and remains a vital driver of change around the world, particularly in societies that lack political rights and press freedom.”