Tightening the Net: Governments Expand Online Controls

FREEDOM ON THE NET 2014
This report was made possible by the generous support of the Dutch Ministry of Foreign Affairs, the U.S. State Department’s Bureau of Democracy, Human Rights and Labor (DRL), Google, and Yahoo. The content of this publication is the sole responsibility of Freedom House and does not necessarily represent the views of the Dutch Foreign Ministry, DRL, Google, or Yahoo.

Cover: Photo from an antigovernment protest outside the ruling party’s headquarters in Bangkok, Thailand on November 29, 2013. Photo: Shutterstock.
Tightening the Net: Governments Expand Online Controls
By Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong

Internet freedom around the world has declined for the fourth consecutive year, with a growing number of countries introducing online censorship and monitoring practices that are simultaneously more aggressive and more sophisticated in their targeting of individual users.

In a departure from the past, when most governments preferred a behind-the-scenes approach to internet control, countries are rapidly adopting new laws that legitimize existing repression and effectively criminalize online dissent.

As a result, more people are being arrested for their internet activity than ever before, online media outlets are increasingly pressured to censor themselves or face legal penalties, and private companies are facing new demands to comply with government requests for data or deletions.

Some states are using the revelations of widespread surveillance by the U.S. National Security Agency (NSA) as an excuse to augment their own monitoring capabilities, frequently with little or no oversight, and often aimed at the political opposition and human rights activists.

The growing restrictions at the national level are also changing the nature of the global internet, transforming it from a worldwide network into a fragmented mosaic, with both the rules and the accessible content varying from one country to another.

Blocking and filtering—once the most widespread methods of censorship—are still very common, but many countries now prefer to simply imprison users who post undesirable content, thereby deterring others and encouraging self-censorship. This approach can present the appearance of a technically uncensored internet while effectively limiting certain types of speech. Meanwhile, physical violence against internet users appears to have decreased in scope.

In 2013, Freedom House documented 26 countries where government critics and human rights defenders were subjected to beatings and other types of physical violence in connection with their online activity; that number fell to 22 in 2014.
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 is the fifth in its series and focuses on developments that occurred between May 2013 and May 2014. The previous edition, covering 60 countries, was published in October 2013. *Freedom on the Net 2014* assesses a greater variety of political systems than its predecessors, while tracing improvements and declines in the countries examined in previous editions. 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, 36 have experienced a negative trajectory since May 2013. Of the 65 countries assessed, 36 have experienced a negative trajectory since May 2013. The most significant declines were in Russia, Turkey, and Ukraine. The Russian government took multiple steps to increase control over the online sphere, particularly in advance of the Sochi Olympic Games and during the ongoing crisis in Ukraine. In Turkey, the blocking of social media, limits on circumvention tools, cyberattacks against opposition news sites, and assaults on online journalists were among the most prominent threats during the year. Ukraine’s standing declined primarily due to violence targeting social-media users and online journalists during the Euromaidan protests, an increase in cyberattacks, and new evidence revealing the extent to which the administration of ousted president Viktor Yanukovych had been conducting online surveillance of activists, journalists, and opposition leaders.

Iran, Syria, and China were the world’s worst abusers of internet freedom overall. Users in China were intimidated and arrested during crackdowns on online “rumors” as President Xi Jinping consolidated control over social media. In September 2014, the same month that students in Hong Kong used the world’s third-fastest internet connection to mobilize prodemocracy demonstrations, mainland courts sentenced prominent Uighur academic and webmaster Ilham Tohti to life imprisonment, the harshest punishment for online dissent in years. Syria was the most dangerous country in the world for citizen journalists, with dozens killed in the past year, while progovernment hackers reportedly infected 10,000 computers with malware disguised as warnings against potential cyberattacks. And despite early enthusiasm over the election of reformist president Hassan Rouhani, Iran maintained its position as the worst country for internet freedom in 2014. Authorities continued to hand down harsh punishments, sentencing people to lengthy prison terms for promoting Sufism online, among other digital activities.

Very few countries registered any gains in internet freedom, and the improvements that were recorded largely reflected less vigorous application of existing internet controls compared with the previous year, rather than genuinely new and positive steps taken by the government. The year’s biggest improvement occurred in India, where authorities relaxed restrictions on access and content that had been imposed in 2013 to help quell rioting in northeastern states.

Another country that registered a notable improvement is Brazil, where after years of debate and revision, lawmakers approved a bill known as the Marco Civil da Internet that contains important provisions governing net neutrality and ensuring strong privacy protections. Freedom House also documented an improvement in Belarus, mainly because the political environment was less volatile and the government eased enforcement of some restrictions, even as citizens increasingly used the internet to voice their views.
Russia's score declined by 11 points over the past 5 years. Since Putin's return to the presidency in 2012, the government has enacted multiple laws to block online content, including critical or opposition media outlets. Individuals are subject to prosecution and physical violence for their internet activity and increasingly extensive surveillance of ICTs lacks sufficient judicial oversight.

Turkey declined 13 points as the government increased censorship, granted state agencies broad powers to block content, and charged more people for online expression. With social media growing as a tool for public discourse, authorities have shut down YouTube, Twitter, and other platforms for months—even years—at a time. Online journalists and social media users are increasingly targeted for assault and prosecution.
Major Trends

New Legal Measures Curb Internet Freedom

In December 2013, as antigovernment protesters flooded the streets in Ukraine, Russian president Vladimir Putin signed a bill authorizing the prosecutor general to block any websites hosting “extremist” content or calls to protest, without judicial oversight. The law took effect on February 1, 2014, and was used immediately to crack down on digital media that carried criticism of the Kremlin's policy toward Ukraine. Within six weeks, three major independent news sites were blocked. A strikingly similar law was enacted in Kazakhstan in April, signifying both the spreading influence of repressive models for internet control—a so-called snowball effect—and a growing trend in which governments use the legal system to codify and legitimize their restrictions.

Between May 2013 and May 2014, 41 countries passed or proposed legislation to penalize legitimate forms of speech online, increase government powers to control content, or expand government surveillance capabilities.

Problematic new laws are emerging in democratic and authoritarian countries alike.

While the legal measures adopted in a range of countries were intended to enable the development of information and communication technologies (ICTs) or protect individual rights, they also typically included problematic provisions with explicit restrictions or ambiguous language that could be abusively applied to legitimate online activities. These new rules come at a time when technological innovations are evolving to circumvent older methods of control, such as blocking and filtering.

In late 2013, for example, the research and advocacy group Greatfire.org began hosting content that is banned by the Chinese government on “unblockable” domains owned by Amazon and other major companies, which officials cannot risk censoring because of their large commercial footprint within China. Separately, during the September-October 2014 prodemocracy protests in Hong Kong, concerns that the authorities might shut down telecommunications service led to widespread use of the mobile phone application FireChat, which enabled protesters to communicate through a network of Bluetooth connections.

Unable to keep up with such developments on a purely technical level, authorities are increasingly turning to their legal systems to control online activity. They are moving beyond the online application of existing, generalized tools, such as criminal defamation laws, and crafting new measures that pertain specifically to ICTs.

Problematic new laws are emerging in democratic and authoritarian countries alike. Democratic states have
struggled to draft legislation that adequately balances legitimate priorities like counterterrorism with the protection of citizens’ rights online. Nevertheless, countries with effective democratic institutions allow for public consultation and correction when laws infringe on fundamental freedoms. By contrast, the avenues for review of abusive laws are limited in nondemocratic states, compromised by closed political systems and weak rule of law. In the most extreme cases, authoritarian regimes simply issue executive decrees or regulations that bypass any legislative or judicial oversight.

Most of the restrictive new legal measures documented by Freedom on the Net 2014 fall into the following categories.

**Bans on online dissent:** While some countries opt to create laws with vague language that can be used to stifle dissent when needed, others are much more open about their goal of cracking down on any criticism. In many cases, the penalties for online expression are worse than those for similar actions offline. In July 2013, for example, the Gambian government passed amendments to the Information and Communication Act that specifically criminalized the use of the internet to criticize, impersonate, or spread false news about public officials. Anyone found guilty could face up to 15 years in prison, fines of roughly $100,000, or both—significantly harsher punishments than what the criminal code prescribes for the equivalent offenses offline.

Restrictions targeting expression on social media were particularly draconian in Vietnam. Decree 72, enacted in September 2013, extended prohibitions against political or social commentary from blogs to all social-networking sites. Decree 174, issued that November, introduced fines for spreading antistate propaganda on social media.

**Criminalization of online defamation:** Measures to criminalize defamation online emerged as a prominent trend. In May 2013, the government of Azerbaijan adopted legal measures that expanded criminal defamation to online content, further constraining criticism of government officials in the run-up to the presidential election in October. Criminal defamation laws are especially problematic given the ease with which casual remarks on social-media platforms can be targeted by officials for reprisal. In January 2014, a Zimbabwean user was arrested for calling President Robert Mugabe “an idiot” on his Facebook page.

**Broad national security laws:** Several countries used the pretext of national security to enact legal measures that allowed the potential restriction of legitimate speech online. In Ethiopia, a new cybersecurity law states that “social-media outlets, blogs, and other internet-related media have great capabilities to instigate war, to damage the country’s image, and create havoc in the economic atmosphere of the country.” The law empowers the government to investigate computers, networks, internet sites, radio and television stations, and social-media platforms “for any possible damage to the country’s social, economic, political, and psychological well-being.” In the Middle East, Jordan broadened its definition of illegal terrorist activities to include acts that could damage the country’s relations with foreign countries, including the online publication of critical commentary on foreign leaders.

In some countries, the penalties for online expression are worse than those for similar actions offline.

**Expanded powers for state regulators:** Other legal measures provided government entities with unchecked discretionary authority over online media and speech. In Kenya, a new information and communications law signed in December 2013 gave the government-appointed regulator vaguely defined new powers, including the authority to impose punitive fines on both journalists and media houses for alleged ethical violations. Similarly in Ecuador, the Organic Law on Communications enacted in June 2013 extended the communication regulator’s control over content to “all media with an online presence.” It was immediately applied to target numerous print and online news outlets.

**Content blocking without a court order:** Measures that empowered government agencies to block content without judicial oversight and with little or no transparency were especially notable in five countries—Turkey, Thailand, Russia, Kazakhstan, and Italy. In the less democratic countries, these laws have coincided with political turmoil and an urgent government desire to suppress dissent.

In Turkey, after audio recordings implicating high-level officials in a corruption scandal were leaked on YouTube and SoundCloud, new legal measures
empowered the state regulator to block websites without a court order in cases that violate privacy or are considered “discriminatory or insulting.” The regulator later blocked YouTube to suppress an unverified recording of a national security meeting. Twitter was also blocked after refusing to suspend user accounts. President Recep Tayyip Erdoğan, who was prime minister at the time, has vowed to “wipe out Twitter” and called social media the “worst menace to society.”

In Thailand, judicial oversight is legally required when web content is blocked, but court orders from the past year undermined that requirement, allowing information officials to block web pages that are “similar” to those specified in the order without seeking separate permission. The situation worsened following the May 2014 coup, as military leaders issued censorship directives under martial law, blocking more than 200 pages in the week after they seized power.

**Excessive intermediary liability:** Some new laws imposed criminal liability on intermediaries—for objectionable content posted by others through their services. In Uganda, the controversial Anti-Pornography Act adopted in February 2014 imposed criminal penalties on service and content providers whose systems are used to upload or download broadly defined “pornographic” material. Although the law was annulled in August on a technicality, it was representative of a broader international trend in which companies or individuals face prosecution merely for providing a platform or network to be used by others.

Of the 65 countries studied in *Freedom on the Net* 2014, 19 passed new legislation that increased surveillance or restricted user anonymity, including authoritarian countries where there is no judicial independence or credible legal recourse for users whose rights have been violated. In April 2014, for example, Turkey passed amendments to the law on the National Intelligence Organization that further insulated the agency’s activities from judicial or media scrutiny. The changes empower the intelligence service to obtain information and electronic data from public bodies, private companies, and individuals without a court order.

The governments of Uzbekistan and Nigeria both passed laws that require cybercafés to keep a log of their customers, and in the case of Uzbekistan, owners must also keep records of customers’ browsing histories for up to three months. In Russia, the so-called “bloggers law,” passed in May 2014, increased government oversight of social-media users by requiring anyone whose sites or pages draw over 3,000 daily viewers to register with the telecommunications regulator.

More democratic countries also drafted, and in some cases passed, potentially harmful surveillance legislation. Despite a significant outcry in France over revelations that the national intelligence agency had been cooperating with the NSA and its British counterpart, in December 2013 the French legislature added an article to an omnibus bill on the military budget that extended the authorities’ legal powers to access or record telephone conversations, e-mail, internet activity, personal location data, and other electronic communications. The legislation provides for no judicial oversight and allows electronic surveillance for a broad range of purposes, including “national security,” the protection of France’s “scientific and economical potential,” and prevention of “terrorism” or “criminality.”

Efforts to reform surveillance legislation in the United States gained momentum in the aftermath of the NSA revelations, though at the end of the period covered by this report, legislative changes were still pending. Notably, some of the bills drafted in Congress would have essentially codified existing surveillance practices. However, by mid-2014 one of the more positive bills, the USA Freedom Act, had garnered significant support from lawmakers, civil society, and the intelligence community.

**Intrusive surveillance:** Following the revelations about NSA surveillance practices, some governments have been working to pass legislation that will improve surveillance policies by balancing the needs of intelligence agencies with the protection of users’ rights. However, other states have enacted laws that further restrict individuals’ ability to communicate anonymously, a trend that is particularly concerning in countries where surveillance is regularly used to monitor and punish dissent.
**Arrests and Reprisals Increase for Social-Media Users**

In tandem with the growing number of legal measures designed to restrict online speech, more people were detained or prosecuted for their digital activities in the past year than ever before. Since May 2013, arrests for online communications were documented in 38 of the 65 countries studied in *Freedom on the Net 2014*, with social-media users identified as one of the main targets of government repression.

Nowhere was this more prevalent than in the Middle East and North Africa. Of the 11 countries examined in the region, 10 featured detentions or interrogations of internet users during the coverage period. Dozens of social-media users were arrested in Bahrain, Saudi Arabia, and the United Arab Emirates, with many sentenced to jail terms of up to 10 years. Despite their high levels of access, the countries of the Persian Gulf remain some of the most restrictive for online freedom of expression.

Social-networking sites—the new battleground for governments seeking to quell protests and organized dissent—spurred an unprecedented volume of legal and extralegal detentions. Chinese police detained hundreds of Weibo microblog users, and indicted some of the most prominent, after top legal authorities established 5,000 views or 500 reposts as a new threshold for prosecuting false, defamatory, or “harmful” comments online. China has imprisoned more internet users than any other nation even without this new justification. The change, however, gave authorities an additional tool to punish dissidents, while also serving as a warning to celebrity bloggers with millions of followers, including members of the business elite. Venture capitalist Charles Xue appeared handcuffed on state television in September 2013 to apologize for sharing unverified information online.

Officials in 11 countries took steps to proactively monitor social media for signs of dissent and to crack down on users for political or social commentary. In Ethiopia, where one blogger is serving an 18-year sentence and six more face trial, the government’s Information Network Security Agency began scanning social media for “damage” to the country’s “well-being” under a November 2013 decree. Also that month, Bahrain’s state media announced the establishment of a Cyber Safety Directorate to monitor websites and social media for content that threatens the unity and cohesion of Bahraini society or that incites violence and hatred.

**More people were detained or prosecuted for their digital activities in the past year than ever before.**

Government attention and reprisals often focused on social-media posts about political leaders. In Bangladesh, supporters of Prime Minister Sheikh Hasina accused their opponents of defaming her on Facebook. In South Korea, where defamation comes with a longer sentence when committed on the internet, at least three people faced trial for online comments about President Park Geun-hye. In some countries, these developments have coincided with the growth of online platforms and their user base.

**Online Journalists and Bloggers Face Greater Pressure**

The past year featured increased government pressure on independent news websites, which had previously been among the few unfettered sources of information in many countries. Bloggers and online journalists covering antigovernment demonstrations faced arbitrary detention and, at times, physical violence at the hands of police or progovernment thugs. Dozens of citizen journalists were killed in Syria, and an independent reporter was fatally shot while covering an antigovernment demonstration in Egypt. Citizen journalists covering mass protests in Turkey and Ukraine were also physically assaulted. Online journalists were arrested in 7 out of 12 sub-Saharan African countries examined in *Freedom on the Net 2014*.

Authorities in Jordan, Singapore, and Russia introduced, updated, or enforced rules mandating that news sites and popular blogs obtain licenses or register with the government, a trend that may inhibit independent reporting given the fear of government retribution. In addition to licensing requirements,

http://www.freedomhouse.org
authoritarian governments used a variety of laws to arrest and intimidate government critics who publish stories online. In Morocco, Ali Anouzla, the Arabic editor of the news site Lakome, was arrested for inciting terrorism after he published an article that contained a hyperlink to a Spanish news site, which in turn had embedded an extremist propaganda video. Lakome was subsequently blocked in one of Morocco’s first cases of politically motivated blocking in years.

In Iran, 16 employees of the gadget review site Narenji were arrested over alleged links to foreign governments and “anti-Iranian media.”

Online journalists and others who publish independent reporting online were arrested in at least 25 countries during the coverage period. In Ethiopia, six writers from the Zone9 news blog were arrested in April 2014 and face charges related to accepting foreign funding and inciting violence through social media. In Iran, 16 employees of the gadget review site Narenji were arrested over alleged links to foreign governments and “anti-Iranian media,” with some apparently charged due to their participation in training programs run by the Persian service of the British Broadcasting Corporation (BBC), which the Iranian government linked to the British intelligence agency M16. Eleven of the defendants were later found guilty, and the website’s founder received the heaviest sentence—11 years in prison.

At times, authorities used trumped-up charges with no link to actual reporting to punish independent journalists. In Uzbekistan, Sergey Naumov, an independent journalist who has contributed reporting for the Ferghana News website, was arrested in September 2013 on charges of hooliganism and given a 12-day jail sentence after he allegedly collided with a woman on the street, who then accused him of harassing her. The charges came days after Naumov began recording video about forced labor practices during the country’s annual cotton harvest. In Azerbaijan, several news site editors were also arrested on apparently fabricated charges of drug possession or hooliganism. In Belarus, a blogger who exposed police corruption was forced to undergo a psychiatric evaluation and faced harassment by police. And in Vietnam, lawyer and blogger Lê Quôc Quân was sentenced to 30 months in prison for tax evasion, a charge that is frequently used by the government to silence dissidents. He had been arrested in 2012, shortly after publishing an article on the website of the BBC’s Vietnamese service.

Civil society activists who use ICTs to document abuse or rally supporters, or simply as a part of their daily lives, also faced threats. Two senior members of Odhikar, a nongovernmental organization (NGO) in Bangladesh, were arrested and charged under the ICT Act for “fabricating” reports of a government crackdown on protesters to “enrage” the public. Alaa Abd el-Fattah, a prominent Egyptian blogger and activist, was sentenced to 15 years in prison in June 2014 for organizing a protest against military trials for civilians. He was not allowed to attend his own sentencing. Although he was released on bail pending a retrial, he was later rearrested. Abd el-Fattah has faced legal harassment from every Egyptian regime since that of former president Hosni Mubarak.
Emerging Threats

In addition to the clear infringements on internet freedom caused by the proliferation of restrictive laws and the rise in arrests and attacks on users and online journalists, Freedom House has identified three emerging threats that are placing the rights of internet users at increasing risk:

- Data localization, by which private companies are required to maintain data storage centers within a given country to allow for greater government control
- A harsh environment for women and members of the LGBTI (lesbian, gay, bisexual, transgender, and intersex) community, who are both underrepresented online and disproportionately harassed for their online activities
- Lack of cybersecurity for human rights activists and political opposition members, who have increasingly been targeted with technical attacks and spying by repressive governments

Data Localization

As governments search for ways to maintain or expand their jurisdiction over the online sphere, internet companies are finding themselves under increasing pressure, whether through court decisions that increase intermediary liability or through government decisions to block access to their platforms. Within this broader trend, proposed data localization requirements—obliging companies to store communications data on servers located within the country in question—have multiplied over the past year, in some cases gaining traction due to the NSA revelations. While these policies could create prohibitive barriers for companies seeking to operate in certain countries, they also pose significant threats to internet users’ rights and ability to access information, for instance by potentially limiting users’ choice of internet platforms and subjecting them to more surveillance by their own governments.

Over the past year, the Russian government has significantly stepped up efforts to exert control over the internet, partly by attempting to regulate the flow of data itself. A law signed in July 2014 requires internet companies to store Russian citizens’ data on servers in Russia. An amendment in September moved up the compliance date from September 1, 2016, to January 1, 2015, which could present a significant challenge for companies like Facebook and Twitter that do not currently have servers within the country. Many human rights advocates are concerned that the new law will make it even easier for Russian intelligence agencies to access the communications data of Russian users, particularly activists and opposition figures who may then face arrests and prosecution for their online activities.

In July 2013, the Vietnamese government issued Decree 72, which, among other things, requires international internet companies to establish at least one server in the country, subject to local law and oversight. Despite the fact that numerous international organizations criticized the original draft of the decree...
as a significant threat to free speech and privacy, the revised drafts maintained the data localization requirement, though it remains unclear how or whether it will be enforced.

Many governments are understandably concerned about how their citizens' information makes its way in and out of other countries' jurisdictions, as the data may be subject to surveillance abroad. But given the decentralized structure of the internet, data localization requirements alone will not prevent crucial information from flowing across borders. Indeed, authoritarian regimes seem to be using these policies for other goals, ranging from enhanced domestic surveillance to reduced competition for domestic internet companies. While data localization may succeed in boosting the economic success of local data centers, they could also have costly effects for other domestic businesses that rely on foreign internet companies.

H **arassment of Women and LGBTI Users**

Internet freedom is particularly tenuous for LGBTI people and women. Globally, women continue to face immense cultural and socioeconomic barriers to ICT access, resulting in a significant gender gap in ICT use. While increasing access to digital media has helped women to fight for political, social, and economic equality, closing the digital gender gap is not enough to guarantee women's participation in the online sphere. Increasingly, women around the world are subject to harassment, threats, and violent attacks for their online activities, which can lead to self-censorship among female internet users and significantly inhibit their freedom of expression.

Internet freedom is particularly tenuous for LGBTI people and women.

In some countries where fundamental rights for women are routinely flouted, they are increasingly targeted for merely accessing ICTs. In Pakistan, a woman was stoned to death by local men in June 2013 after a tribal court convicted her of possessing a mobile phone. Also that month, a group of men fatally shot a woman and her two daughters in the country's north after a video of the women laughing, which male family members considered shameful, circulated on local mobile networks.

In Azerbaijan, investigative journalist Khadija Ismayilova has repeatedly been subjected to blackmail and gender-based smear campaigns in an attempt to silence her and discredit her work. In India, women's rights activist Kavita Krishnan was harassed online by a person using the handle "@RAPIST." Digital activists were also penalized for documenting violence against women: Mukhlif al-Shammar was jailed for five years in June 2013, in part for posting a YouTube video on the mistreatment of girls in Saudi Arabia.

Members of the LGBTI community have faced targeted threats and harassment via ICTs, impeding their ability to freely use certain tools. In Egypt, there were reports that the authorities used the dating application Grindr to entrap and prosecute gay men. Following the adoption of Uganda’s Anti-Homosexuality Act in February 2014, numerous members of the LGBTI community reported receiving e-mail spyware known as “Zeus malware” that sought to access their contact details and confidential information from compromised computers. Similarly in Russia, where the parliament passed a law against LGBTI “propaganda” in June 2013, vigilante groups used online tools to bait gay men, luring them to in-person encounters where they were physically assaulted and threatened with public exposure.

**Lack of Cybersecurity**

As users have become more privacy conscious, malware attacks against government critics and human rights organizations have evolved to take on a more personalized character. Technical attacks against such targets were noted in 32 of the 65 countries examined this year.

So-called spear phishing has emerged as one of the most effective techniques for hijacking online accounts and collecting sensitive information. Victims receive customized e-mail messages that typically direct them to an official-looking page, run by the hackers, where they are prompted to enter their e-mail or social-media credentials. These sorts of attacks were employed by the Syrian Electronic Army against international news organizations such as the New York Times, Global Post, CNN, and Forbes over the past year.
Once in control of an opposition website or social-media account, hackers can post hyperlinks to online petitions or exciting news stories to lure users into clicking. These links often have hidden tracking capabilities that can ascertain a user’s location. According to a report by BahrainWatch, malicious links have been used to identify and arrest several anonymous Twitter users who were outspoken against the government in that country. The increased use of “social engineering”—essentially tricking users into revealing information—and account hijacking has reinforced the idea that one’s own digital security often depends on the actions and judgment of those in one’s broader social or professional network.

In many cases, assailants perform substantial research about a target’s interests, professional connections, and personal relationships in order to create an individually tailored attack. For instance, bogus Facebook, Google, LinkedIn, and Twitter profiles have been set up by Iranian intelligence agents to “friend” foreign targets. One LinkedIn profile under the name of John Bolton, the former U.S. ambassador to the United Nations, was created to ensnare pro-Israel researchers and exiled members of Iran’s persecuted Baha’i community. Attackers sometimes spend several months building trust before sending a link to a relevant news story that contains malicious code.

Spear-phishing victims are often prompted to download a particular file that then installs a malware program. Hackers using this technique have targeted members of the Ethiopian exile community, such as opposition figure Tadesse Kersmo and staff at the Virginia-based news outlet ESAT. Researchers at the University of Toronto’s CitizenLab have traced the attacks to individuals working for or in close coordination with the Ethiopian government.

In Pakistan, a woman was stoned to death by local men in June 2013 after a tribal court convicted her of possessing a mobile phone.

The Ethiopian example reflects a growing trend in which progovernment hackers are expanding their operations beyond national borders. In one case, attackers hijacked the prodemocracy site of a Vietnamese blogger living in California and used it to publish her personal photos and e-mails. Researchers noted that the malware employed was detectable by only 1 in 47 antivirus programs at the time, reflecting an unusually high level of sophistication that suggested state involvement.
The Global Struggle for Internet Freedom

Despite overall declines in global internet freedom, an ongoing trend of pushback from civil society was amplified this year by reactions to the NSA surveillance revelations. Awareness of the threats to fundamental rights expanded beyond civil society, as ordinary users around the world became more engaged in securing their privacy and freedom of expression online. In select cases, long-running internet freedom campaigns finally garnered the necessary momentum to succeed.

The most widely praised step forward for internet freedom over the past year was the passage of Brazil’s Marco Civil da Internet, thanks in large part to pressure from activists and the public. The bill, which had stalled in Congress after numerous debates and revisions, gained fresh traction following the disclosure that the NSA and other intelligence agencies had engaged in mass collection and storage of the communications data of users around the world. The widespread alarm inspired potentially negative revisions to the bill, such as data localization requirements, but these were ultimately removed. In a more positive response to the NSA scandal, a Brazilian legislator included even stronger privacy provisions for user data. The final bill also contains key provisions restricting traffic discrimination in order to guarantee net neutrality, and ensuring strong protections for freedom of expression online. While there are still some problems with the final text, including the mandatory retention of access data for six months, the Marco Civil was widely regarded as a positive example for other countries.

Popular uproar over government surveillance had a positive effect elsewhere in Latin America, where problematic proposals were halted. In Ecuador, lobbying efforts by the Internet Libre collective resulted in the defeat of Article 474 of the penal code, which would have forced ISPs to record all user activity for six months. In Argentina, community members prevented a government initiative to proactively monitor social-networking sites for potentially disruptive events, which opponents deemed “preemptive surveillance.”

In Europe, outrage over the NSA revelations brought the topic of user privacy to the center of discussions in the European Parliament and EU member states. In December 2013, the European Court of Justice ruled that current requirements placed on ISPs to indiscriminately store data on their customers were in contravention of Articles 7, 8, and 52(1) of the Charter of Fundamental Rights of the European Union. Civil society critics had long argued that the requirements of the European Data Retention Directive constituted mass surveillance and far exceeded what was necessary for law enforcement purposes. However, the decision to strike down the directive has prompted a range of reactions among the member states, with some drafting their own retention laws to ensure that ISPs continue to store user data.

These legislative and judicial successes notably occurred in democratic states, where the rule of law prevails and governments are generally held accountable to citizens and civil society. In Brazil, for
example, the draft of the Marco Civil was the result of a collaborative process that included input from civil society and ordinary citizens, and it had support from members of Congress and the president.

In more authoritarian settings, and in democracies where needed reforms are still pending, individuals and companies have taken matters of privacy and freedom of expression into their own hands by using anonymizing and encryption tools. Products that emphasize user privacy have logged a notable increase in users since June 2013. On the anniversary of the NSA revelations, civil society campaigns placed an emphasis on educating users about available privacy tools. And internet companies that initially came under fire for cooperating with intelligence agencies or not adequately protecting user data have since taken steps to improve their encryption standards.

Internet freedom is important not just for its own sake, but because it facilitates expression and activism on other issues. Civil society organizations have continued to use ICTs to advocate for positive change in their communities, such as the recognition of women’s rights in the Middle East. In Lebanon, online campaigns by the NGOs Nasawiya and Kafa contributed to the passage of a law on domestic violence. Since a 2013 UN report found that over 99 percent of Egyptian women had experienced sexual harassment, websites such as Harassmap have spread awareness about the issue while providing tools for victims to report incidents and obtain psychological or legal support. In Saudi Arabia, a campaign to allow women to drive cars gained momentum after a dozen women posted videos of themselves driving in a coordinated day of action in October 2013.

In these and a growing number of other countries, the internet is a crucial medium not just for personal communication or news and information, but for political participation and civic engagement. The struggle for internet freedom is consequently inseparable from the struggle for freedom of every kind.
### Key Internet Controls by Country

<table>
<thead>
<tr>
<th>Country (by FOTN 2014 ranking)</th>
<th>FOTN 2014 Status (F=Free, PF=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>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 for political or social writings</th>
<th>Online journalist/blogger/ICT user physically attacked or killed (including in custody)</th>
<th>Technical attacks against government critics and human rights organizations</th>
<th>TOTAL # of Key Internet Controls employed in 2013-2014, by country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iceland</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>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>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>F</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Germany</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>United States</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>France</td>
<td>F</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>Italy</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Japan</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Hungary</td>
<td>F</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Georgia</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>South Africa</td>
<td>F</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Argentina</td>
<td>F</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Phillipines</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Armenia</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Kenya</td>
<td>F</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Brazil</td>
<td>F</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Colombia</td>
<td>F</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>Nigeria</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>South Korea</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Ukraine</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Uganda</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>Ecuador</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Angola</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Mexico</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Tunisia</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Singapore</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>India</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Indonesia</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Malawi</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Malaysia</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Country (by FOTN 2014 ranking)</td>
<td>FOTN 2014 Status (F=Free, PF=Partly Free, NF=Not Free)</td>
<td>Social media and/or communications apps blocked</td>
<td>Political, social, and/or religious content blocked</td>
<td>Localized or nationwide Internet shut down</td>
<td>Pro-government commentators manipulate online discussions</td>
<td>New law/directive increasing censorship or punishment passed</td>
<td>New law/directive increasing surveillance or restricting anonymity passed</td>
<td>Online journalist/blogger/ICT user arrested for political or social writings</td>
<td>Online journalist/blogger/ICT user physically attacked or killed (including in custody)</td>
<td>Technical attacks against government critics and human rights organizations</td>
<td>TOTAL # of Key Internet Controls employed in 2013-2014, by country</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------</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>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>2</td>
</tr>
<tr>
<td>Morocco</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>4</td>
</tr>
<tr>
<td>Cambodia</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1</td>
</tr>
<tr>
<td>Lebanon</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>4</td>
</tr>
<tr>
<td>Jordan</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>3</td>
</tr>
<tr>
<td>Libya</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>2</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>4</td>
</tr>
<tr>
<td>Rwanda</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>5</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>7</td>
</tr>
<tr>
<td>Turkey</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>7</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>4</td>
</tr>
<tr>
<td>Venezuela</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>8</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1</td>
</tr>
<tr>
<td>Egypt</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>5</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>6</td>
</tr>
<tr>
<td>Myanmar</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>4</td>
</tr>
<tr>
<td>Russia</td>
<td>PF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>7</td>
</tr>
<tr>
<td>Belarus</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>4</td>
</tr>
<tr>
<td>Thailand</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>6</td>
</tr>
<tr>
<td>Sudan</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>5</td>
</tr>
<tr>
<td>The Gambia</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>6</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>4</td>
</tr>
<tr>
<td>Pakistan</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>6</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>7</td>
</tr>
<tr>
<td>Bahrain</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>6</td>
</tr>
<tr>
<td>Vietnam</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>7</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>6</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>7</td>
</tr>
<tr>
<td>Cuba</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>5</td>
</tr>
<tr>
<td>China</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>8</td>
</tr>
<tr>
<td>Syria</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>6</td>
</tr>
<tr>
<td>Iran</td>
<td>NF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>6</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td>17</td>
<td>34</td>
<td>13</td>
<td>24</td>
<td>21</td>
<td>19</td>
<td>38</td>
<td>22</td>
<td>32</td>
<td></td>
</tr>
</tbody>
</table>
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.

---

65 Country Score Comparison

**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 House

http://www.freedomhouse.org
Map of Internet Freedom
Freedom on the Net 2014 assessed 65 countries around the globe. The project is expected to expand to more countries in the future.

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>FREE</td>
<td>19</td>
</tr>
<tr>
<td>PARTLY FREE</td>
<td>31</td>
</tr>
<tr>
<td>NOT FREE</td>
<td>15</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>65</strong></td>
</tr>
</tbody>
</table>
Regional Graphs

*Freedom on the Net 2014 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.*
Internet Freedom vs. Press Freedom

Digital media in several of the 65 countries covered was relatively unobstructed when compared to the more repressive or dangerous environment for traditional media. This difference is evident from the comparison between a country’s score on Freedom House’s Freedom on the Net 2014 and Freedom of the Press 2014 assessments.

The figure above shows the 37 countries in this edition with a score difference of 10 points or greater. The bar graph characterizes a country’s Freedom on the Net 2014 score, while the scatterplot (■) represents the country’s score in Freedom of the Press 2014, which measures media freedom in the broadcast, radio, and print domains. This difference is cause for concern. Pressures that constrain expression in print or broadcast formats have the potential to exert a negative impact, in the short or long term, on the space for online expression.
The figure above depicts the relationship between internet penetration rates and the level of digital media freedom in Freedom on the Net 2014. Each point reflects a country's internet penetration rate, as well as its overall performance in the rest of the survey.

The **PARTLY FREE** countries in the middle are particularly noteworthy. As digital access increases, they have a choice—to move right, and join the countries that are high-tech but **NOT FREE**; or left, with the **FREE** countries that better protect expression.
### Freedom on the Net 2014: Overview of Score Changes

<table>
<thead>
<tr>
<th>Country</th>
<th>FOTN 2013</th>
<th>FOTN 2014</th>
<th>Overall Trajectory</th>
<th>FOTN 2014 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>Asia</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bangladesh</td>
<td>49</td>
<td>49</td>
<td>Partly Free</td>
<td>12</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Cambodia</td>
<td>47</td>
<td>47</td>
<td>Partly Free</td>
<td>14</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>China</td>
<td>86</td>
<td>87</td>
<td>▼</td>
<td>Not Free</td>
<td>19</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>India</td>
<td>47</td>
<td>42</td>
<td>▲</td>
<td>Partly Free</td>
<td>13</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Indonesia</td>
<td>41</td>
<td>42</td>
<td>▼</td>
<td>Partly Free</td>
<td>11</td>
<td>▲</td>
<td>▼</td>
</tr>
<tr>
<td>Japan</td>
<td>22</td>
<td>22</td>
<td>Free</td>
<td>4</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Malaysia</td>
<td>44</td>
<td>42</td>
<td>▲</td>
<td>Partly Free</td>
<td>8</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Myanmar</td>
<td>62</td>
<td>60</td>
<td>▲</td>
<td>Partly Free</td>
<td>19</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Pakistan</td>
<td>67</td>
<td>69</td>
<td>▼</td>
<td>Not Free</td>
<td>20</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>Philippines</td>
<td>25</td>
<td>27</td>
<td>▼</td>
<td>Free</td>
<td>10</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>Singapore</td>
<td>*</td>
<td>40</td>
<td>▼</td>
<td>Partly Free</td>
<td>6</td>
<td>*</td>
<td>▼</td>
</tr>
<tr>
<td>South Korea</td>
<td>32</td>
<td>33</td>
<td>▼</td>
<td>Partly Free</td>
<td>3</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>58</td>
<td>58</td>
<td>Partly Free</td>
<td>15</td>
<td>▼</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>Thailand</td>
<td>60</td>
<td>62</td>
<td>▼</td>
<td>Not Free</td>
<td>11</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>Vietnam</td>
<td>75</td>
<td>76</td>
<td>▼</td>
<td>Not Free</td>
<td>14</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td><strong>Eurasia</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Armenia</td>
<td>29</td>
<td>28</td>
<td>▲</td>
<td>Free</td>
<td>7</td>
<td>▲</td>
<td>9</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>52</td>
<td>55</td>
<td>▼</td>
<td>Partly Free</td>
<td>14</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>Belarus</td>
<td>67</td>
<td>62</td>
<td>▲</td>
<td>Not Free</td>
<td>15</td>
<td>▼</td>
<td>▲</td>
</tr>
<tr>
<td>Georgia</td>
<td>26</td>
<td>26</td>
<td>Free</td>
<td>8</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>59</td>
<td>60</td>
<td>▼</td>
<td>Partly Free</td>
<td>15</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>35</td>
<td>34</td>
<td>▲</td>
<td>Partly Free</td>
<td>12</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Russia</td>
<td>54</td>
<td>60</td>
<td>▼</td>
<td>Partly Free</td>
<td>10</td>
<td>▼</td>
<td>▲</td>
</tr>
<tr>
<td>Turkey</td>
<td>49</td>
<td>55</td>
<td>▼</td>
<td>Partly Free</td>
<td>14</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>Ukraine</td>
<td>28</td>
<td>33</td>
<td>▼</td>
<td>Partly Free</td>
<td>8</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>78</td>
<td>79</td>
<td>▼</td>
<td>Not Free</td>
<td>20</td>
<td>▼</td>
<td>▼</td>
</tr>
<tr>
<td><strong>Latin America</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td>27</td>
<td>27</td>
<td>Free</td>
<td>7</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Brazil</td>
<td>32</td>
<td>30</td>
<td>▲</td>
<td>Free</td>
<td>7</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Colombia</td>
<td>*</td>
<td>30</td>
<td></td>
<td>Free</td>
<td>8</td>
<td>*</td>
<td>▲</td>
</tr>
<tr>
<td>Cuba</td>
<td>86</td>
<td>84</td>
<td>▲</td>
<td>Not Free</td>
<td>23</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Ecuador</td>
<td>37</td>
<td>37</td>
<td>Partly Free</td>
<td>9</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Mexico</td>
<td>38</td>
<td>39</td>
<td>▼</td>
<td>Partly Free</td>
<td>10</td>
<td>▲</td>
<td>▼</td>
</tr>
<tr>
<td>Venezuela</td>
<td>53</td>
<td>56</td>
<td>▼</td>
<td>Partly Free</td>
<td>17</td>
<td>▼</td>
<td>▼</td>
</tr>
</tbody>
</table>

* Overall trajectories for the five new countries were based on a retroactive analysis of internet freedom for those countries.

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.
<table>
<thead>
<tr>
<th>Country</th>
<th>FOTN 2013</th>
<th>FOTN 2014</th>
<th>Overall Trajectory</th>
<th>FOTN 2014 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>Overall</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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>72</td>
<td>74</td>
<td>▼</td>
<td>Not Free</td>
<td>12</td>
<td>▼</td>
<td>27</td>
</tr>
<tr>
<td>Egypt</td>
<td>60</td>
<td>60</td>
<td></td>
<td>Partly Free</td>
<td>15</td>
<td>12</td>
<td>33</td>
</tr>
<tr>
<td>Iran</td>
<td>91</td>
<td>89</td>
<td>▲</td>
<td>Not Free</td>
<td>22</td>
<td>▲</td>
<td>31</td>
</tr>
<tr>
<td>Jordan</td>
<td>46</td>
<td>48</td>
<td>▼</td>
<td>Partly Free</td>
<td>12</td>
<td>▲</td>
<td>15</td>
</tr>
<tr>
<td>Lebanon</td>
<td>45</td>
<td>47</td>
<td>▼</td>
<td>Partly Free</td>
<td>14</td>
<td>▼</td>
<td>12</td>
</tr>
<tr>
<td>Libya</td>
<td>45</td>
<td>48</td>
<td>▼</td>
<td>Partly Free</td>
<td>18</td>
<td>▼</td>
<td>9</td>
</tr>
<tr>
<td>Morocco</td>
<td>42</td>
<td>44</td>
<td>▼</td>
<td>Partly Free</td>
<td>11</td>
<td>▼</td>
<td>10</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>70</td>
<td>73</td>
<td>▼</td>
<td>Not Free</td>
<td>15</td>
<td>▼</td>
<td>24</td>
</tr>
<tr>
<td>Syria</td>
<td>85</td>
<td>88</td>
<td>▼</td>
<td>Not Free</td>
<td>25</td>
<td>▼</td>
<td>26</td>
</tr>
<tr>
<td>Tunisia</td>
<td>41</td>
<td>39</td>
<td>▲</td>
<td>Partly Free</td>
<td>11</td>
<td>▲</td>
<td>8</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>66</td>
<td>67</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>34</td>
<td>38</td>
<td>▼</td>
<td>Partly Free</td>
<td>15</td>
<td>7</td>
<td>▼</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>79</td>
<td>80</td>
<td>▼</td>
<td>Not Free</td>
<td>23</td>
<td>▼</td>
<td>28</td>
</tr>
<tr>
<td>Gambia, The</td>
<td>*</td>
<td>65</td>
<td>▼</td>
<td>Not Free</td>
<td>19</td>
<td>*</td>
<td>21</td>
</tr>
<tr>
<td>Kenya</td>
<td>28</td>
<td>28</td>
<td></td>
<td>Free</td>
<td>9</td>
<td>7</td>
<td>12</td>
</tr>
<tr>
<td>Malawi</td>
<td>42</td>
<td>42</td>
<td></td>
<td>Partly Free</td>
<td>16</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>Nigeria</td>
<td>31</td>
<td>33</td>
<td>▼</td>
<td>Partly Free</td>
<td>10</td>
<td>▼</td>
<td>8</td>
</tr>
<tr>
<td>Rwanda</td>
<td>48</td>
<td>50</td>
<td>▼</td>
<td>Partly Free</td>
<td>12</td>
<td>▼</td>
<td>19</td>
</tr>
<tr>
<td>South Africa</td>
<td>26</td>
<td>26</td>
<td></td>
<td>Free</td>
<td>7</td>
<td>8</td>
<td>11</td>
</tr>
<tr>
<td>Sudan</td>
<td>63</td>
<td>65</td>
<td>▼</td>
<td>Not Free</td>
<td>18</td>
<td>▼</td>
<td>19</td>
</tr>
<tr>
<td>Uganda</td>
<td>34</td>
<td>34</td>
<td></td>
<td>Partly Free</td>
<td>11</td>
<td>7</td>
<td>▲</td>
</tr>
<tr>
<td>Zambia</td>
<td>*</td>
<td>43</td>
<td>▼</td>
<td>Partly Free</td>
<td>12</td>
<td>*</td>
<td>13</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>54</td>
<td>55</td>
<td>▼</td>
<td>Partly Free</td>
<td>15</td>
<td>▲</td>
<td>15</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>17</td>
<td></td>
<td>Free</td>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>Canada</td>
<td>*</td>
<td>15</td>
<td>▼</td>
<td>Free</td>
<td>3</td>
<td>*</td>
<td>3</td>
</tr>
<tr>
<td>Estonia</td>
<td>9</td>
<td>8</td>
<td>▲</td>
<td>Free</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>France</td>
<td>20</td>
<td>20</td>
<td></td>
<td>Free</td>
<td>3</td>
<td>▲</td>
<td>4</td>
</tr>
<tr>
<td>Germany</td>
<td>17</td>
<td>17</td>
<td></td>
<td>Free</td>
<td>4</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>Hungary</td>
<td>23</td>
<td>24</td>
<td>▼</td>
<td>Free</td>
<td>5</td>
<td>8</td>
<td>11</td>
</tr>
<tr>
<td>Iceland</td>
<td>6</td>
<td>6</td>
<td></td>
<td>Free</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Italy</td>
<td>23</td>
<td>22</td>
<td>▲</td>
<td>Free</td>
<td>4</td>
<td>▲</td>
<td>6</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>23</td>
<td>24</td>
<td>▼</td>
<td>Free</td>
<td>2</td>
<td>6</td>
<td>16</td>
</tr>
<tr>
<td>United States</td>
<td>17</td>
<td>19</td>
<td>▼</td>
<td>Free</td>
<td>4</td>
<td>2</td>
<td>▼</td>
</tr>
</tbody>
</table>
65 Country Reports
Angola

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>6</td>
<td>7</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>38</td>
</tr>
</tbody>
</table>

Population: 21.6 million
Internet Penetration 2013: 19 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Two individuals were charged with defamation for their alleged ties to articles posted on the independent news website, Club-K (see Violations of User Rights).
- Evidence from inside sources affirmed that a German company had assisted the Angolan military intelligence in installing a sophisticated communications monitoring system on a military base. Further evidence, as of November 2013, found that at least one major ISP hosts a spyware system directly on its server (see Violations of User Rights).
- A prominent investigative journalist was arrested while interviewing protesters for his independent news blog in September 2013; he was also the target of a sophisticated and customized malware attack on his computer that was traced to parties within the Angolan government (see Violations of User Rights).
Introduction

The Angolan government has invested heavily in improving access to information and communication technologies (ICTs) since 2005. Today, Angola boasts one of the largest mobile telecommunications markets in sub-Saharan Africa, and internet access is growing steadily. In 2013, Angola implemented the Strategic Plan for E-Governance for 2013-2017, which outlined the government’s commitment to e-governance initiatives.\(^1\) In its 2014 state budget, the government allocated over US$267.3 million for the development, upgrade, and maintenance of the technological infrastructure for central and provincial e-government web portals, more than doubling the 2013 ICT budget of US$100 million.\(^2\)

Despite progress in ICT development, internet freedom in Angola is tenuous. 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 34 years. 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 for unspecified content under the Electronic Communications and Information Society Services’ Law, enacted in 2011.

While internet content and communications applications are freely accessible, the government seems increasingly intent on cracking down against online dissent through legal and extralegal means. In June 2013, the Attorney General’s Office charged two individuals with abuse of the press and defamation for their alleged association with Club-K, an independent news portal operated by the Angolan diaspora. Travel bans were imposed on the individuals until pressure built on social media succeeded in overturning the restrictions.

Meanwhile, insider sources established that the Angolan military intelligence had implemented an electronic monitoring system for the tracking of email and other digital communications sometime in late 2013. Further evidence, as of November 2013, found that at least one major ISP hosts a spyware system directly on its server. In addition, harassment, extralegal violence, and technical attacks against online journalists increased during the coverage period, with the prominent investigative journalist Rafael Marques de Morais arrested in September 2013 and beaten while in custody, after being targeted for a customized malware attack on his computer earlier in the year.

Obstacles to 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 2013, the internet in Angola reached a penetration rate of 19 percent, up from 17 percent in 2012,


Angola

according to the International Telecommunications Union (ITU). By contrast, access to mobile phones is much higher with a penetration rate of 62 percent in 2013, up from 49 percent in 2012. Over 12 percent of Angolans have a mobile broadband subscription. Meanwhile, fixed-line broadband subscriptions remain very low with a penetration rate of only 0.2 percent in 2013, and are largely concentrated in the capital city, Luanda, due to the country’s high poverty rate and poor infrastructure in rural areas.

Luanda is reputed to be the second most expensive city in the world, and for those able to access the internet in urban areas, internet 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. Already expensive for the vast majority of Angolans, whose median annual per capita income is US$720 according to a 2013 Gallup study, voice and data services in rural areas 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. Due to these high prices, most internet users log online at their workplaces.

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. Consequently, 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.

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. In early 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.\textsuperscript{15} Construction of SACS is expected to be completed by mid-2015.\textsuperscript{16}

Broadband connection speeds in Angola are still slow, averaging 1.5 Mbps (compared to a global average of 3.9 Mbps), according to May 2014 data from Akamai’s “State of the Internet” report.\textsuperscript{17} In addition, Angola’s broadband adoption (characterized by connection speeds greater than 4 Mbps) is only about 3 percent,\textsuperscript{18} while the country’s narrowband adoption (connection speed below 256 kbps) is less than 2 percent.\textsuperscript{19}

The ownership structure of internet service providers in Angola enables the government via senior officials who double as businesspersons to control internet services through their direct and indirect shareholder participation in many Angolan companies. 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.\textsuperscript{20} The national telecom company, Angola Telecom, an ISP itself, is also a major shareholder in Angola Cables, with 51 percent.\textsuperscript{21}

Two private operators, UNITEL and Movicolor, provide mobile services,\textsuperscript{22} though both telecoms have indirect ownership ties to the government. For example, 75 percent of UNITEL, the larger mobile phone operator, is held by three entities: the state oil company, Sonangol; a business venture\textsuperscript{23} 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.\textsuperscript{24} Meanwhile, 80 percent of Movicolor 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 presidential office. For example, the majority shareholders of the Angolan investment company Lambda include the Minister of Telecommunications and Information Technologies José

\begin{itemize}
  \item \textsuperscript{15} Estefania Jover et al., “Angola, Private Sector Country Profile.”
  \item \textsuperscript{20} 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, n° 17, Sonangol.
  \item \textsuperscript{21} Angola Cables is a joint venture by the five main telecom operators in the country, established to manage and control Angola’s participation (11.4 percent) in the West Africa Submarine System (WACS), as well as the national teleport. It commercializes access to fiber submarine cables for international voice and data circuits.
  \item \textsuperscript{22} Instituto Angolano das Comunicações (INACOM), “Statistics,” accessed July 31, 2014, http://www.inacom.og.ao/Publi-ca%C3%A7%C3%B5es/Estat%C3%ADsticas.aspx.
  \item \textsuperscript{23} The investment company: Portmill, Investimentos e Telecomunicações.
\end{itemize}
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.

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, the welfare of citizens, competitiveness, productivity, employment, territorial and cultural cohesion, social inclusion and consumer rights. Nevertheless, this legislation includes several provisions that constitute serious threats to online freedom. For one, although the law provides for universal access to information through cyberspace, universal access is dependent upon the state’s responsibility “in the creation and promotion of conditions that enable all citizens to access ICT.” The law accordingly enables the president as 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.

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. 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.

---

27 Assembleia Nacional, Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação (Lei nº 23/11), Art. 5.
28 Assembleia Nacional, Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação (Lei nº 23/11), Art. 14º, a), k), 2011.
29 Ibid., Art. 15º.
30 Ibid., Art. 5º.
31 Ibid. Art. 26º, 2.
Limits on Content

During the coverage period, online self-censorship became more prevalent, reinforced by recent attacks on online journalists. One online news portal reported receiving calls from government officials to self-censor on certain topics.

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, aside from child pornography and copyrighted material. 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 affect the internet. The president and members of the ruling 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.

Self-censorship is pervasive and commonly practiced by journalists in both state-run and private print outlets, though there is more open criticism of the president and ruling party circulating on blogs and social media platforms. 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 in 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 “Violations of User Rights”). In addition, taboo topics related to corruption, abuse of power, land grabs, police brutality, and demolitions are often avoided.

Independent news outlets that are critical of the government do exist, with Folha8 being the most prominent, though its audience is reached primarily through its print publication. A new portal based in Portugal launched in 2013, Rede Angola, has become one of the main sources of alternative and independent online news on Angola, though according to internal sources, the portal has been subject to censorship calls. For example, in May 2013, Rede Angola’s newsroom

---

37 Based on interviews with internet users and bloggers.
38 Rede Angola website: http://www.redeangola.info/
39 Based on information from internal sources at Rede Angola disclosed to the author.
Angola reportedly received instructions from the management not to publish any news on the kidnappings and torture of more than 20 protesters by the Angolan Rapid Intervention Police on May 27, 2013.40

The economic viability of independent outlets, both online and 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.41 Moreover, 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.

Meanwhile, Angola has seemingly embraced e-governance initiatives and is known as the first country in sub-Saharan Africa to pass an access to information law in 2002. In 2014, most ministries and provinces have their own web portals, and a citizen’s portal, Cidadao.gov.ao, exists to facilitate the provision of public services to society. In practice, however, there is still a dearth of information and services that citizens can access through government portals, which essentially serve as a repository of state media news on related departments.42

In addition, numerous government websites are infrequently updated and often lack both basic and essential information. The website of the vice president, Manuel Vicente, for example, does not disclose his biography,43 while the ministry of telecommunications and ICT, which is in charge of e-government projects, has not updated its public agenda on its website since May 2012,44 posting solely news events. Journalists have found it baffling that the current minister of information, José Luís de Matos, has not published his biographical information on the ministry’s portal, except the date of his appointment in October 2013.45 Meanwhile, the presidential website has been “temporarily unavailable” since 2012.46

Another aspect of the government’s mediocre engagement with the internet is its inability to interact with citizens through social media. While the government’s main portal links to social media accounts on Facebook, YouTube, Twitter, and Flickr, the accounts are rarely updated, likely due to an unwillingness to employ full-time censors to monitor and moderate public comments, according to some analysts. Consequently, the government’s apparent investments in e-governance and ICTs have not guaranteed more access to information or enhanced citizens’ participation in decision-making processes as promised. It has also failed to foster government accountability and transparency, and improve interactions between public officials and citizens.

Nevertheless, social media has become the leading platform for citizens to criticize the government

---

42 The citizen’s portal does not provide any direct or indirect online services but only basic information on bureaucratic requirements on how and where to apply for ID’s, driver’s licenses, and death certificates. It mostly provides addresses to services in the capital, Luanda, although it claims nationwide coverage.
and react to alleged wrongdoings. Youth groups have increasingly flocked to Facebook to call for protests against government corruption, reflecting a weakening culture of fear within civil society. In June 2013, when two individuals were issued travel bans after being indicted for their alleged association with the independent news website, Club-K (see “Violations of User Rights”), activists on social media played a significant role in pressuring the government to overturn the travel restrictions. Online protests and mobilization efforts, however, have yet to result in major political or social outcomes.

Violations of User Rights

During the coverage period, the police and public magistrates began aggressively prosecuting individuals specifically for their online activities for the first time. Two individuals were charged with abuse of the press and defamation for their suspected ties to the diaspora web portal, Club-K. Evidence from investigative research affirmed that a German company had assisted the Angolan military intelligence in installing a sophisticated communications monitoring system on a military base. Further evidence, as of November 2013, found that at least one major ISP hosts a spyware system directly on its server. In September 2013, two journalists were arrested while interviewing protesters for the independent news blog Maka Angola and were beaten while in custody.

The Angolan constitution provides for freedom of expression and the press, though in practice, these constitutional rights are routinely flouted by the government and authorities. Meanwhile, 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.47 The 2006 press law holds authors, editors or directors of a publication criminally liable for libelous content.48 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.49 Defamation is also a crime punishable by imprisonment, while politicians enjoy complete immunity.

In 2002, Angola became one of the first African countries to enact a freedom of information law. In practice, however, accessing government information remains extremely difficult. The judiciary is subject to considerable political influence, with Supreme Court justices appointed to life terms by the president and without legislative oversight. Nevertheless, the courts have been known to rule against the government on occasion.50

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.\(^{51}\) Nevertheless, a draft Cybercrime Law (short for the Law to Combat IT, Communications and Information Society Services’ Crimes) introduced in May 2011 attempted to provide the government with legal measures to circumvent a slew of users’ rights online and penalize certain online activities.\(^{52}\) For example, Article 16 of the draft law would increase penalties prescribed for offenses laid out under Angola’s criminal code—such as defamation, libel, and slander—committed via electronic media, thereby penalizing online conduct offenses more harshly than offline.\(^{53}\)

Introduced by the president’s office to the National Assembly in March 2011,\(^{54}\) the law was ultimately withdrawn in May 2011 as a result of internal pressure and vocal objections from civil society.\(^{55}\) Nonetheless, a government minister publicly stated the same year that special clauses regarding cybercrimes would instead be incorporated into an ongoing revision of the penal code,\(^{56}\) leaving open the possibility of internet-specific restrictions coming into force in the future.\(^{57}\) Meanwhile, the government has publicly stood by the constitutionality of the draft Cybercrime Law’s controversial clauses.\(^{58}\)

In recent years, a number of journalists in the traditional media sphere have been prosecuted for criminal defamation in lawsuits initiated by government officials.\(^{59}\) Most recently, two individuals

---


\(^{52}\) If the draft law had passed, the law would also have empowered the authorities with the ability to intercept information from private devices without a warrant and prosecute individuals for objectionable speech expressed via ICTs and on social media platforms. Sending an electronic message interpreted as an effort to “endanger the integrity of national independence or to destroy or influence the functionality of state institutions” would have yielded a penalty of two to eight years in prisons, in addition to fines. The law would have further criminalized the dissemination of any “recordings, pictures and video” of an individual without the subject’s consent, even if produced lawfully, which could have impeded journalists’ ability to report on public protests or instances of police brutality using digital tools. The bill additionally prescribed penalties between 8 and 12 years in prison for espionage and whistle blowing activities, which would have included the act of seeking access to classified information on an electronic system “in order to reveal such information or to help others to do so.” The same penalty was provided for accessing unclassified information that could be deemed as endangering state security. See: “Angola: Withdraw Cybercrime Bill,” Human Rights Watch, May 13, 2011, [http://www.hrw.org/news/2011/05/13/angola-withdraw-cybercrime-bill](http://www.hrw.org/news/2011/05/13/angola-withdraw-cybercrime-bill).

\(^{53}\) The draft would also make it illegal to post online or to share photos, recordings or videos without the consent of those appearing in the content. Those found guilty could serve from two to eight years in jail, though all state institutions, including the state media, would be exempt from this legal demand. This would make it illegal to use social media to post photographs, videos or even to publish satirical images of the president and members of the regime without their consent. The government also wants to punish those who send or forward messages (email, text, tweet, etc.) that might “disturb the peace and tranquility or the personal, familiar or sexual life of another person.” See: “Angola: Withdraw Cybercrime Bill,” Human Rights Watch, May 13, 2011, [http://www.hrw.org/news/2011/05/13/angola-withdraw-cybercrime-bill](http://www.hrw.org/news/2011/05/13/angola-withdraw-cybercrime-bill); Assembleia Nacional, Proposta de Lei de Combate à Criminalidade no Domínio dos TIC e dos Serviços da Sociedade da Informação, 2010.


\(^{56}\) The revised Penal Code has been in limbo for passage into law since 2006. It incorporates the abovementioned controversial articles of the Cybercrime Law into its penal sanctions within the framework of defamation. Ministério da Justiça e dos Direitos Humanos, Anteprojecto de Código Penal, Arts. 200, 201. [www.safili.org/pt/legis/num_act/cp76.pdf](http://www.safili.org/pt/legis/num_act/cp76.pdf).


were prosecuted for their alleged ties to the diaspora web portal Club-K, the popular independent news website hosted abroad by members of the Angolan diaspora. On July 9, 2013, the Attorney General’s Office charged José Gama and Lucas Pedro Fenguele, a journalist and an activist, for crimes of abusing the press, defamation, and slander against senior public officials based on two articles published in Club-K, despite the fact that there was no evidence the individuals had been responsible for either of the two articles. The first article alleged that the Attorney General of the Republic, General João Maria de Sousa, owned a mansion in Portugal. The second was merely a post of an article originally published by the Portuguese weekly newspaper Expresso on investigations that General de Sousa had been facing in Portugal for money-laundering and fraud. As of mid-2014, the authorities have kept the suspects in a judicial limbo without any further information on the case.

There are no restrictions on anonymous communication such as website or SIM card registration requirements. Nevertheless, in April 2013, a Club-K investigative report revealed that intelligence and state security services were allegedly planning 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). In early 2014, a follow up investigation by an anonymous researcher found corroborating information from military sources, affirming that a German company had indeed assisted the Angolan military intelligence in installing a sophisticated monitoring system at the BATOPE base around September 2013. There was further evidence, as of November 2013, of at least one major ISP hosting a spyware system directly on its server, as part of the German company setup.

The blurred lines between the public and private sectors in Angola make it difficult to ascertain the extent to which the government needs to require ICT providers to assist in the monitoring of communications. 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 Movitel. The deputy CEO and Chief Technology Officer of Unitel, Amílcar Safeca, is the brother of Aristides Safeca, the secretary of the state for ICT who in turn is a shareholder of Movitel. Such interweaving of political and family connections with the private sector, the researcher claimed, “My clients are neither editors of Club-K nor authors of the articles. Lucas Pedro is a freelance writer and José Gama is simply an activist.” See: “José Gama Interditado de Sair do País,” Maka Angola, August 2013, http://makaangola.org/2013/08/23/jose-gama-interditado-de-sair-do-pais/.


5 General Kopelipa openly represents Portmill, Investimentos e Telecomunicações, which holds 40 percent of Movitel. He is also a co-owner of Banco Espírito Santo Angola which is a major Movitel 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.
interests of the same individuals is compounded by the lack of a rule of law. As a result, the strong presence of the state in the 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 if desired. Cybercafes, however, are not known to be subject to such requirements.

Attacks and extralegal violence against journalists in the traditional media sphere are unfortunately common in Angola, and online journalists are increasingly targeted. In one notable incident on September 20, 2013, journalist Rafael Marques de Morais and Alexandre Solombe, a colleague who was assisting him, were arrested while interviewing protesters for the independent news blog, Maka Angola. They were beaten while in custody, threatened until they relinquished their mobile phone PIN numbers, and subsequently released without charges. Marques de Morais’s mobile phone was returned damaged beyond use, and the police kept the memory card with over 1,000 pictures and videos. Several months later, the journalist discovered that Minister of the Interior Ângelo de Barros Tavares had personally ordered the operation. According to the Marques de Morais’s sources, the main objective of the operation was to seize his digital equipment for clues to his government sources who were suspected of leaking information to the Maka Angola news blog.

Independent and diaspora news websites have also been subject to technical violence, such as hacking and denial-of-service (DoS) attacks, particularly during periods of political contestation. For example, in 2013, the personal laptop belonging to journalist Rafael Marques de Morais was attacked with customized malware. Tests later conducted on his computer found that the surreptitious malware worked by taking screenshots of Marques de Morais’s computer activity every 20 seconds and transferring the images to a server in India. An international expert, Jacob Appelbaum, traced the author of the malware to an Indian national. Appelbaum also found that the Portuguese franchise of a Western multinational doing business in Angola with strong ties to some of the above-mentioned generals had solicited the spyware service.

Argentina

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>8</td>
<td>7</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>27</td>
<td>27</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 41.3 million

Internet Penetration 2013: 60 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: No

Bloggers/ICT Users Arrested: No

Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- In February 2014, Argentina’s Supreme Court ruled that the government—which has ignored a string of previous directives—must comply with equitable allocation of advertising. The government’s refusal to do so has jeopardized the existence of independent online media outlets, which, like mainstream media, rely heavily on advertising revenue to sustain daily operations (see Limits on Content).

- In late 2013 and early 2014, a handful of contradictory court cases impacted Argentine standards for intermediary liability, specifically regarding whether intermediaries, including search engines, are required to monitor their platforms for illegal or restricted content (see Limits on Content).

- In December 2013, Juan Pablo Suarez, editor of the online news site Ultima Hora, was detained for nine days for filming the arrest of a local police officer (see Violations of User Rights).

- In July 2013, the Secretariat of Communications issued Resolution 5/2013, the vague wording of which could infringe on users’ right to privacy by potentially allowing unfettered access to telecommunications infrastructure and user data (see Violations of User Rights).

- In October 2013, a glitch in the online electoral system enabled the photos of some registered voters to be downloaded by others, violating data protection and privacy standards (see Violations of User Rights).
Editor's Note:

In late 2014, members of the Argentine National Congress began working on legislation to replace the 1972 Telecommunications Law. Drafts of the proposed “Argentina Digital” bill, which the government submitted to congress in October 2014 and which was subsequently debated and revised throughout November, have contained worrisome provisions related to internet freedom. While the principle of net neutrality was strengthened through revisions to the bill, there remain serious concerns over the amount of power given to the regulatory authority, appointed directly by the executive branch and authorized to grant or deny licenses to ICT companies, broadly defined. As this report was published, however, legislation has yet to be passed.

Introduction

Internet penetration has increased at a steady rate since 2009, due in part to government policies aimed at improving service and expanding broadband connections throughout the country. Argentina now has one of the largest contingents of internet users in South America, and many initiatives aimed at increasing internet access, such as the Argentina Connected Plan, have already demonstrated success. The government’s latest statement reveals that 15,453 kilometers of fiber-optic cables have already been built for Argentina’s backbone, and infrastructure use agreements have been made with various telephone companies to facilitate internet access.

Although the Argentine legal framework protects free speech online and offline, in recent years, a number of judicial decisions have negatively impacted the availability of online content. Between 2010 and 2013, several court judgments restricted access to websites on claims of defamation or intellectual property rights violations, with one ruling leading to the accidental blocking of the entire blog-hosting platform Blogger.

Personal data is generally protected by article 43 of the constitution; however, a handful of recent events may be cause for concern. A July 2013 resolution issued by the Communications Secretariat that regulates quality requirements for telecommunications services contains vague wording regarding government access to infrastructure, which could endanger privacy given its potential for broad interpretation. In October 2013, a serious breach of internet user privacy and anonymity occurred when a glitch in the online electoral system allowed citizens’ photos to be downloaded. Recent projects intended to combat online child pornography and cybercrimes against children through the implementation of “child grooming” laws have also sparked criticism for overly broad language. Two worrying initiatives pertaining to the regulation of social media were also launched recently in the province of Entre Ríos and the city of La Plata.

During 2013 and 2014, many bills were discussed in Congress regarding high-stakes internet challenges such as intermediary liability and net neutrality. The lack of a specific framework for the

former has led to diverse case law in Argentina, and has, at times, resulted in orders specifying the deletion of content. A new controversial regulation, enacted in March 2014, also requires annual fees for the registration of domain names.

The Argentine government has a long record of discriminatory distribution of official advertising, creating economic obstacles for critical media outlets. Despite multiple court rulings mandating fair and equitable allocation, discriminatory practices have continued.\(^5\)

### Obstacles to Access

Over the past decade, internet access has consistently been on the rise in Argentina, with the International Telecommunication Union (ITU) measuring the internet penetration rate at 60 percent in 2013, compared to 56 percent in 2012 and just 28 percent in 2008.\(^6\) According to Argentina’s national statistics institute, INDEC, as of September 2013 there were 12.4 million residential subscriptions, the majority of which were broadband; only 35,975 subscriptions were for dial-up connections. By September 2013, INDEC also counted 2.3 million organizations with internet subscriptions (a 20 percent increase over the previous year), 537 of which benefited from free internet access. Those institutions benefitting from free access included schools, libraries, and nongovernmental organizations.\(^7\)

Continuing expansion of internet access is a key facet of Argentina’s development strategy. In April 2013, legislation was passed guaranteeing access to web content for people with disabilities.\(^8\) Law 26.653, which concerns access to public information, was amended to comply with fair and equal treatment for the disabled, extending access provisions to this portion of the population.\(^9\) In May 2013, Argentine newspaper *La Nación* published a map of Buenos Aires identifying locations with free public Wi-Fi, such as hospitals, museums, libraries, and theaters.\(^10\)

Measurements of Argentina’s average internet speed have varied considerably, making it difficult to get an accurate reading. In February 2014, Netflix ranked the country among the slowest at both the regional and global levels, with speeds of 1.2 to 1.88 Mbps depending on the internet service provider (ISP), figures that come in below Akamai’s reading of 2.7 Mbps for the third quarter of

---


2013. By contrast, a study from the University of San Andrés measured speeds of 7 Mbps in the metropolitan area, with speeds decreasing in rural areas and provinces. Argentina currently has ten functioning Network Access Points (NAPs) to help with traffic.

In Argentina, the state does not set the price of internet subscription fees. According to the ITU, the average broadband plan costs US$36.50 per month, which represents 4.5 percent of the country's gross domestic product. In October 2013, Hernán Galperín, Director of the Technology and Society Centre of San Andrés University, published a report stating that Argentina's cheapest internet access plan is among the most expensive in the region. Accordingly, affordability is one of the most significant obstacles in Argentina, and has been cited by a reported 56 percent of Argentines as the reason they lack internet access.

Argentina also suffers from infrastructural weaknesses that limit internet penetration throughout the country, particularly in rural areas. Connectivity of both residential and organizational subscriptions is concentrated in urban areas, with the majority of both types found in Buenos Aires, Córdoba, Santa Fe, and Mendoza. In order to address such regional disparities, the government has begun promoting different policies such as the Argentina Connected Plan (Argentina Conectada), Connect Equality (Conectar Igualdad), and the Digital Agenda (Agenda Digital), each of which aims to remedy a different facet of the problem.

The Argentina Connected Plan, a five-year initiative created in 2010, is defined as an “integral connectivity strategy” that aims to “generate a digital platform of infrastructure and services.” One of the initiative’s most important components is the Federal Network of Optical Fiber (Red Federal de Fibra Óptica), a project that is employing 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 to 97 percent of the population. In response to concern over the pace of the project's development, a

---


16 Galperín, Hernán, Broadband Prices in Latin America and the Caribbean, UDESA. Figure 1, p6, http://www.udesa.edu.ar/files/AdmTecySociedad/15%20Gaperin-%20Enq.pdf.


18 For information on connections, please see: http://www.indec.mecon.ar/nuewweb/quadros/14/internet_12_13.pdf

19 CELE’s Translation: http://www.argentinaconectada.gob.ar/contenidos/que_es_argentina_conectada.html

2013 report assured the public that construction of the fiber-optic cable was on track.\(^1\) Recent government disclosures have further revealed that 15,453 km of cable has already been built, with an additional 4,500 km of existing infrastructure purchased and further contracts signed with telephone companies assuring use of their infrastructure.\(^2\)

The Connect Equality initiative—another positive government program begun in 2010—aims to foster digital inclusion by providing a netbook to every student and teacher in public high schools.\(^3\) As of February 2014, more than 3.8 million netbooks had been delivered. The Digital Agenda initiative, created in 2009, is also dedicated to facilitating access to ICTs for social connection and development.\(^4\) The website Educ.ar further aims to expand opportunities for and equality in education by granting access to digital platforms that host educational content.\(^5\)

As of mid-2014, these policies have resulted in increasing internet access in rural areas, schools, parks, and public spaces.\(^6\) Some provinces have also made arrangements with the national government to build a wider fiber-optic network, which is being installed by rural cooperatives. These projects have begun to show significant growth in local penetration rates and are allowing provincial governments to plan for future “triple play” service.\(^7\) Discussions have also arisen regarding the availability of “quad play” service (a bundled service package of broadband internet, television, and telephone, along with wireless service provisions) in the near future. It is in this context that the government has deemed the Federal Wireless Network an issue of public interest,

---


a classification which will prioritize the expansion of national internet access. In keeping with its growing ICT investment, the Argentine government has already built two communications satellites, one of which, Arsat-1, is expected to be launched between August and September 2014; the other, Arsat-2, will be launched in 2015.

There are approximately 300 licensed ISPs in Argentina, indicating 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 ARS 5,000, a fairly reasonable amount considering that the average monthly wage is ARS 7,500.

Mobile phone penetration has also grown consistently in Argentina in recent years. According to the ITU, as of November 2013, there were nearly 66 million mobile phones actively in use, indicating an increase of over 1.5 million subscriptions from the previous year. The licensing process for mobile phone providers is similar to that for ISPs; once approved, no additional fees are charged, although providers are required to pay special taxes, such as those specified under the Universal Service Trust Fund. Cybercafe licenses are processed like those of any other small business with no additional requirements.

In 2004, the government confiscated bands of the radio spectrum after mobile company Movícom was sold to Telefónica (Telefónica was forced to relinquish the frequencies to avoid concentration of the spectrum). After repeatedly postponing legal hearings, President Kirchner announced that Libre.ar—a branch of state-owned company AR-SAT—would administer the frequencies. This decision was implemented through Resolution 71/2012 of the Communication Secretariat and justified with the rationale that only one of the companies bidding for the bands met necessary requirements.
related to future investment and development. The decision also allowed the government to regain control over the mobile sector, though fortunately such control has not extended to the government overtaking ICTs.

As a result of the decision, Libre.ar will hold 25 percent of the radio spectrum and will provide mobile services through small companies and cooperatives across the country. This plan will encourage cooperatives to resell services, a development they view as an opportunity to gain recognition in the mobile services arena. The new plan is also attractive to foreign investors looking to enter Latin America’s mobile market, such as Chinese telecommunications firm Datang Mobile, which views Argentina as the most profitable point of entry due to its large number of cell phones and potential to embrace 4G services, which have yet to be launched.

The national regulatory body that oversees digital technology—the CNC—was founded as a relatively independent, public, decentralized body, whose functions are to regulate and supervise ICTs. A 2002 presidential decree intended to increase efficiency, however, may have detracted from the body’s independence by granting the executive the power to appoint an intermediary. This intervention is ongoing, and may contribute to public mistrust of the regulator.

**Limits on Content**

In February 2014, Argentina’s Supreme Court ruled that the government must comply with equitable allocation of advertising. Additionally, in late 2013 and early 2014, a handful of contradictory court cases impacted standards for intermediary liability, specifically regarding the liability of search providers for removing content containing the unauthorized use of individual’s images.

---


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. Although there is no automatic filtering of internet sites, web pages, blogs, or data centers, Law 25.690 tasks ISPs with the duty to provide software that limits access to specific websites. Law 2974 also mandates the blocking of websites related to pornography in educational institutions, libraries, and other public locations in Buenos Aires. Similar laws have been enacted in some of the provinces, such as Santa Fe.

YouTube, Facebook, Twitter, and international blog-hosting services are freely available in Argentina, although social media sites have occasionally been blamed for coordinating vandalism and other illegal activities. In December 2013, Minister of Justice Julio Alak stated that a wave of looting that occurred in Entre Ríos and other Argentine provinces had been organized through social media in response to a police protest. Consequently, in Entre Ríos there was a proposal to limit the use of social networks. The proposed resolution stated that it was necessary to block “comments, expressions, and information that fosters ‘apología’ [incitement] of criminal acts and violence…” Although this would have been a blow to freedom of expression, the initiative was severely criticized and the project did not succeed.

According to Google’s Transparency Report, from January to June 2013, the Argentine government submitted 35 court orders as well as 6 executive or police orders for content removal. Although the number of requests declined from the previous term, the amount of content covered in these requests increased greatly, encompassing 1,748 items. By contrast, from July to December 2012, 51 orders for content removal were issued, encompassing only 160 items. Although this increase is due in part to a court order requesting the removal of 1,385 search results (Google did not remove these results, but instead appealed the order, which was then reversed), excluding that particular order, the

---

51 Infobae, “El Texto de La Resolución que Prohíbe el Uso de Twitter y Facebook Durante Crisis Sociales” [The Text of the Resolution that Forbids the Use of Twitter and Facebook During Social Crisis], Infobae, December 18, 2013, http://www.infobae.com/2013/12/18/1531720-el-texto-la-resolucion-que-prohíbe-el-uso-twitter-y-facebook-durante-crisis-sociales
number of items still doubled in the first half of 2013. In both the 2012 and 2013 terms, the majority of the content was related to defamation.53

Among the most salient issues likely to impact internet access in Argentina are net neutrality regulation and intermediary liability. The Senate Commission of Systems, Media, and Freedom of Expression debated various projects related to these issues throughout 2013.54 One of the more positive aspects to Resolution 5/2013, issued by the Secretariat of Communications, specifically provides for net neutrality, mandating that providers "guarantee access to every user, that in no way distinguishes, blocks, interferes, discriminates, hinders, degrades or restricts arbitrarily the reception or sending of information."55

In recent years, controversy has emerged in Argentina over the blocking of allegedly defamatory material, copyright protected content, and injunctions that invoke intermediary liability. In October 2012, for example, a judge ordered the CNC to mandate that ISPs block specific websites that explain how to unblock netbooks from the government’s Connect Equality program in order to use them for purposes other than education and digital literacy.56 The most recent—and highly controversial—cases of blocking concerned sites that were illegally commercializing medicine and electronic devices. The National Administration of Public Income (AFIP) blocked 37 such sites in November 2013.57 In December, three additional websites were taken down, allegedly by the National Direction of Registration of Internet Domains (NIC.ar), after a complaint from the National Administration of Medicine, Food and Medical Technology (ANMAT) that the sites were commercializing electronic cigarettes, which are prohibited in Argentina.58 The controversy around these cases stemmed from a lack of clarity over whether the blocks and takedowns were, in fact, court-authorized. In a public statement, ANMAT announced that it had worked with NIC.ar; however, as the agency is an entity of the executive branch and not fully transparent, uncertainty remains over whether a court order preceded the blocking and removal of the content in question.

Cases of blocking on grounds of copyright infringement have also surfaced from time to time. In 2009, a court ordered the blocking of blog Que Te Pasa Clarin because of alleged copyright infringement against newspaper Diario Clarín. Although the ruling was reviewed—and subsequently overturned—by the National Federal Civil Court of Appeals in March 2014, the domain was sold to another individual while it was blocked so that the owner could no longer make use of it. Hence, although the ruling was overturned, the blog no longer exists.

Another important case regarding copyright infringement and intermediaries concerns the popular social platform and content sharing site Taringa. In 2011, copyright complaints were filed against the site—which has over 24 million registered users—by the nonprofit organization Cámara Argentina del Libro (CAL) and several editors. In response, the National Court of Criminal Appeals prosecuted the owners as “necessary participants” in the violations committed by their subscribers, who used Taringa! to share content protected by copyright law. Although the Supreme Court confirmed the prosecution in August 2012, in March 2013 both parties reached an agreement under which they would create a mechanism for CAL to monitor content shared over the platform. Although this decision sparked criticism because it would entail content monitoring by private entities, it was nonetheless approved.

To date, there is no specific legislation regarding intermediary liability in Argentina. Due to the absence of specific regulation, judicial rulings adjudicating liability to intermediaries or injunctions ordering them to remove content are based on general rules, and decisions tend not to be uniform. In 2013, numerous rulings regarding intermediary liability were issued, some of which were positive, exempting hosting companies from disproportionate measures, and some of which were negative, applying overly broad consumer protections that negatively impact the function of search engines. In one late 2013 case, which had a positive ruling from a freedom of expression standpoint, the production company Pampa Films filed a criminal lawsuit against YouTube administrators, Google, and a YouTube user for allowing the movie “Un Cuento Chino” to be uploaded without legal permission and hosted on YouTube. The movie, which was viewed by nearly 200,000 people in the nine months it was available, was removed by the company after complaints from Pampa Films. The First Instance Criminal Court and the Criminal Court of Appeals each ruled that YouTube could
not be held criminally liable for hosting the film since it does not prescreen content uploaded by users, and praised the company for responding to the complaint by removing the content in question.66

A handful of cases pertaining to the unauthorized use of images or videos have also come to the fore in recent years. In one 2010 case, the artist Virginia Da Cunha sued Google and Yahoo for the unauthorized use of her image by websites that offered sexual services. The National Civil Court of Appeals ruled that intermediaries could only be held liable if they were nonresponsive to complaints, establishing a subjective liability regime, under which liability is assigned if an actor is deemed negligent. Although the case is awaiting a ruling by the Supreme Court, in August 2013, the Attorney General issued an opinion confirming the ruling made by the Appeals Court, which stated that satisfying Da Cunha’s request would be tantamount to requiring pre-emptive censorship.67 This is a positive ruling for freedom of expression as it requires companies to respond to complaints but does not force intermediaries to monitor content as it is created, which could place undue burdens on intermediaries and lead them to censor legitimate content in order to limit legal liability.68

Two important rulings issued in 2013 are decidedly less positive for freedom of expression. In the May 2013 case of Florencia Peña, an actress who was victim to the online publication of a stolen video of her and her husband having intimate relations,69 the Court of First Instance issued a precautionary measure ordering Google to block all search results containing the actress’ name along with terms alluding to the video, rather than taking a more nuanced and proportionate precautionary measure such as ordering the blocking of the specific URLs hosting the video. Another example of a ruling with a potentially dangerous precedent occurred in the December 2013 case of Evangelina Carrozo, a model whose image was used without authorization in sexual content websites. In its ruling, the National Civil Court of Appeals tasked Google and Yahoo with the obligation to compensate Ms. Carrozo for the use of her image.70 The Court further stated that search engines carry out an inherently risky activity, making them automatically liable for content.71 The Court’s findings are controversial as they imply that search engines ought to act as arbiters of content. Such responsibility would effectively force intermediaries to engage in censorship, negatively impacting freedom of expression and access to information.72

One March 2014 case stands as a positive counterexample to the concerning ruling in the Carrozo case. In this suit, which also involved a model, Carolina Valeria, whose name and image were used in sexual content websites, the National First Instance Civil Court ruled in favor of Google, the

---

68 In May 2014, the Supreme Court called for an audience in a similar case (video here: http://www.cij.gov.ar/nota-13404-Sequir--este-jueves-la-audiencia-p-blica-de-la-Corte-en-causa-por-responsabilidad-de-buscadores-de-internet.html); Many Amicus Curiae briefs were presented by specialists advising the Court on how to rule. See: Rodriguez, María Belen c/ Google Inc. s/daños y perjuicios.
70 Carrozo, Evangelina c/ Yahoo de Argentina SRL y otro s/ daños y perjuicios: http://www.infojus.gov.ar/jurisprudencia/NV6830-carrozo_yahoo_danos-nacional-2013.htm?sessionid=1vc3ebb7ts1nuv2ndnkpog70
71 See Article 1113 pertaining to objective liability; See also Carrozo, p. 7.
search engine being sued. In his ruling, the judge stated that the company had conducted no illegal behavior, and further, that forcing Google to delete all entries with the model’s name would amount to prior censorship.\(^73\)

Two key legislative proposals that would have limited intermediary liability came to the fore in 2012, although neither was passed. Proposal 2668-D-2012 would have excluded ISPs serving as technical intermediaries from responsibility for content originating from a third party, as long as the ISP did not alter the content in question.\(^74\) After this proposal was rejected in 2012 amidst criticism, its author, Representative Pinedo, updated the draft bill and presented it again; it was rejected a second time in March 2013.\(^75\) The other proposal, 8070-D-2012, would have excluded ISPs from liability for all transmitted information, unless the ISP modified the information or was the original transmitter. This initiative faced criticism for disregarding international standards when allowing third parties and administrative bodies to ask ISPs to remove content without a judicial order.\(^76\)

Self-censorship among bloggers and online users is not widespread in Argentina, yet in the interior of the country, where the rule of law is weaker than in the capital district, some online journalists refrain from writing about powerful local officials so as not to jeopardize their relationship with private advertisers. According to the latest IFEX report, given Argentina’s polarized political and press environment, public media is used as a tool to question journalists who criticize the government.\(^77\) Some writers likewise adjust their reporting based on the partisan affiliation of their publication.

One significant issue facing news outlets is discriminatory allocation of official advertising, a practice for which the Argentine federal and local governments are known. Outlets whose reporting has been critical of the government are often excluded from official advertisement, while those who are supportive are rewarded with reallocation of advertisement opportunities.\(^78\) This biased practice has inhibited freedom of expression, particularly in the print and broadcast media sectors.\(^79\) Although funds allocated to internet activities represent only three percent of the federal advertising budget, the most recent publicly available statistics show that during the first semester of 2012, 42

\(^{73}\) Gimbutas Carolina Valeria c/Google Inc s/Habeas Data and Gimbutas Carolina Valeria c/Google Inc s/danos y perjuicios, http://scw.pjn.gov.ar/scw/viewer.seam?id=jx%2F6uvPA6Y7ssT%2F04x6mo9k77qNgYFb90Mxw0KfKas53D&typeDoc=despacho&cid=455864


\(^{79}\) Poder Ciudadano, “Dimensión de la Publicidad Oficial en la Argentina.”
percent of that sum was assigned to only 10 beneficiaries, all of whom had clear ties to the federal government. 80

Despite multiple rulings by the Supreme Court and the Federal Court of Appeals in 2011 and 2012 stating that the government must utilize equitable measures in its distribution of state advertising, to date, the government has been noncompliant and has faced no penalty for its disregard of judicial orders. 81 In June 2013, the National Civil Court of Appeals made yet another ruling urging the government to distribute official advertising in an equitable and proportional way. 82 In October, the Supreme Court issued a further ruling regarding the constitutionality of the Telecommunications Law in which it recommended “transparent public policy in terms of official advertising.” 83 Finally, in February 2014, the Supreme Court confirmed its ruling urging the government to comply with equitable advertising allocation, emphasizing the importance of this principle to freedom of expression. 84 To date, however, the government does not appear to have changed its stance on equitable allocation of advertising.

There are no restrictions on access to national or foreign news sources in Argentina. Argentines are able to express themselves freely online; in recent years, many have also used social media as a tool for political mobilization. In late 2012, Twitter and Facebook were used to mobilize protestors in a major antigovernment demonstration known as 8N (November 8). Although official figures vary widely, placing the size of the protests between 30,000 (according to the Buenos Aires police) and 100,000 (according to regional media), 8N succeeded in bringing tens of thousands of people out to protest corruption, violent crime, declining freedom of expression, and inflation. 85 In April 2013, another public demonstration known as 18A (April 18) was organized using social media, and, like

---

83 “La Corte Suprema Declaró la Constitucionalidad de la Ley de Medios” [Supreme Court rules Media Law as Constitutional], http://www.cij.gov.ar/nota-12394-La-Corte-Suprema-declar--la-constitucionalidad-de-la-Ley-de-Medios.html.
Argentina

8N, gathered a great deal of attention on Twitter and Facebook.\(^{86}\) According to the Buenos Aires City Government, 18A gathered over 1 million protesters—a figure that was challenged by the National Government, which stated that only 178,000 people attended.\(^{87}\) The 18A protest took place in the capital and in other Argentine cities such as Mar del Plata, Santa Fe, Rosario, and Salta.

A few other notable public demonstrations were also organized via social media during 2013. In October 2013, a march was arranged on social media in support of President Cristina Fernández de Kirchner, who was in the hospital recovering from an operation.\(^{88}\) In December 2013, after suffering multiple power outages due to a heat wave and an energy deficit, social media was widely used as a tool to organize protests. One of the resulting movements, known as 30D, invited citizens to gather on December 30th for a march toward the Obelisc in protest of the power cuts.\(^{89}\) Although the government did not respond to 30D, it stands as an example of the practical use of social media by Argentines as a tool for real-world mobilization.

Violations of User Rights

A number of incidents over the past year threatened internet users’ rights to freedom of expression and privacy online. In December 2013, Juan Pablo Suarez, the editor of the online news site Ultima Hora, was detained for nine days after filming the arrest of a local police officer. In October 2013, a glitch in the online electoral system enabled the photos of some registered voters to be downloaded by others, violating data protection and privacy standards. Additionally, in July 2013, the Secretariat of Communications issued Resolution 5/2013, which could infringe on users’ right to privacy by potentially allowing unfettered access to telecommunications infrastructure and user data.

The Argentine Constitution and human rights treaties incorporated in 1994 guarantee freedom of expression.\(^{90}\) Additional laws also exist to ensure that citizens have the liberty to express their

---


88 Terra Noticias, “Todos con Cristina,” La Convocatoria para El 17 de Octubre” [Everyone with Cristina, the Convocation for October 17th], Terra Noticias, October 16, 2013, http://noticias.terra.com.ar/politica/todos-con-cristina-la-convocatoria-para-el-17-de-octubre.95f82b8b551c1410VgnCLD2000000dc6eb0aRCRD.html; See also; El Intransigente, “Convocan a Apoyar a Cristina Kirchner el 17 de Octubre en Plaza de Mayo” [Convocation to Support Cristina Kirchner on October 17th at Plaza de Mayo], El Intransigente, October 16, 2013, http://www.elintransigente.com/notas/2013/10/16/convocan-apoyar-cristina-kirchner-octubre-plaza-mayo-212160.asp


views without fear of censorship or reprisal, a protection that was extended to the internet in 1997.91 Constitutional protection was also extended to “the search, reception and dissemination of ideas and information of all kinds via internet services” in 2005 under Law 26032.92

The Argentine judiciary is generally seen as independent, particularly in its higher echelons, such as the Supreme Court of Justice. Not all regulatory bodies in Argentina benefit from the same level of autonomy as the judiciary, however. In December 2011, NIC.ar, which regulates and registers domain names, was placed directly under oversight of the executive branch of government, where it remains to this day.93 In late 2012, controversy arose over denials of domain names related to President Cristina Fernández de Kirchner and the progovernment youth group “La Cámpora.”94 Although some blamed the close relationship between NIC.ar and the executive, there is no evidence of similar cases in 2013.

In November 2009, the legislature decriminalized defamatory statements referring to matters of public interest.95 Although there are no specific laws that criminalize online expression related to political or social issues, recent cases have detracted from the ability of reporters to cover the arrest of an elected official—an event that is arguably a “matter of public interest.” In one controversial December 2013 case, Juan Pablo Suarez, the editor of news website Ultima 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.96 During the arrest, police officers also seizing computers and documents from the website’s headquarters.97 While there are no penalties for “irresponsible journalism,” a recent statement by Chief of Cabinet Jorge Capitanich is worrisome. Mr. Capitanich claimed that Vice President Amado Boudou—currently being processed in a criminal case of corruption98—is a victim of “media
A court order is officially required to intercept private communications, even in cases related to national security, a precedent established by Argentina’s National Intelligence Law to ensure user privacy. Such procedures appear to be followed, although there are no official figures detailing the number of annual interceptions. According to Google’s Transparency Report, between January and June 2013, Argentine authorities made 114 requests for user data spanning 132 accounts. Google complied in 48 percent of cases. Microsoft’s Law Enforcement Request Report for the


Argentina

first semester of 2013 states a total number of 455 requests for user data covering 675 accounts. Microsoft complied with 371 requests.106

Argentina tends to hold high privacy and data protection standards, and while there have occasionally been local initiatives aimed at decreasing public unrest via the surveillance of online platforms, to date, none have been put into practice. Following complaints about unruly parties and other events in La Plata, Gustavo Luzardo, sub-secretary of the Urban Control Department, announced that local government would monitor social networks to trace planned events, in order to “advise” neighbors of potentially disruptive events. After allegations by community members and specialists alike that such monitoring would amount to a form of “pre-emptive surveillance,”107 assurances were provided that such measures—which could endanger freedom of expression on social networks—would not be taken.108

Despite a strong data protection framework, in July 2013, the Secretariat of Communications passed a resolution that may impact user privacy. Resolution 5/2013109 governs the quality of telecommunications services and states that providers should “guarantee the free access of the CNC to installations... and [should] give them all the information that is required...”110 Although the resolution mentions respect for personal data, the vague wording has the potential to lead to violations of users’ privacy.111 Additionally, in October 2013, a glitch in the online electoral system sparked significant concern when it enabled the photos of some registered voters to be downloaded by others, violating data protection and privacy standards.112 In response, a local NGO filed a collective habeas data suit—a constitutional legal action that claims that every citizen has the right to see any information concerning himself or herself which appears in the public or private archives, and that he or she may also request the deletion of incorrect or sensitive information. In keeping with this rule, the NGO requested the elimination of citizens’ images from the electoral roll.113 To date, there has been no ruling on this matter, although the online electoral roll is currently inactive.
Although attacks against online journalists occur sporadically, they are not as common as violence against those working for traditional media outlets, which has become a “noticeable problem.”114 According to the Argentine Journalism Forum (FOPEA), there were 194 attacks against 239 journalists in 2013—mainly physical aggression, harassment and censorship—a slight rise as compared to the 172 attacks witnessed in 2012.115 Attacks specifically targeting digital media journalists have proven more difficult to tally with accuracy but appear to have decreased over the past year. Although fear of being attacked could lead to self-censorship, as of mid-2014, it did not appear to be a significant barrier to freedom of online expression. While defamatory campaigns have occasionally targeted bloggers,116 as of June 2014, such incidents did not appear to be widespread or on the rise.

The Argentine government passed a law on cybercrime (Law 26388) in 2008, which amended the Argentine Criminal Code to prohibit distribution and possession of child pornography, interception of communications and informatics systems, hacking, and electronic fraud.117 Some of the terms used in the legislation have been criticized as too ambiguous, which could lead to expansive application of the law. To date, however, this law has not been used to punish online expression. Although cybercrime investigation units do not yet appear to exist on the national level,118 a one-year pilot project aimed at investigating cybercrimes was activated in Buenos Aires in November 2012.119 A 2013 report about the pilot project revealed 172 ongoing cybercrime felony cases, 120 of which correspond to child pornography cases.120

Many draft bills on the issues of child grooming and cybercrime have been presented in Congress in recent years. The most recent bill was aimed at criminalizing electronic contact with minors that may lead to harm of the minor’s sexual integrity.121 This proposal sparked criticism among academics and legislators due to vague wording that would have criminalized any online interaction with minors, issuing the same sentence that is mandated for cases of abuse.122 Despite the criticism, in November 2013, Law 26.904 was passed by the Congress, establishing penalties of six months 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." 123

In July 2011, the Executive Power established the National Program of Critical Infrastructure of Information and Cybersecurity (ICIC). 124 The program, which is comprised of four working groups, aims to create a framework to foster identification and protection of strategic infrastructure. One of its groups aims to reduce security breaches and to minimize information safety risks; another offers assessment when emergencies arise as the result of such incidents.

In August 2013, the official Twitter account of the House of Government, @CasaRosadaAR, was hacked and used to publish offensive posts about a journalist. In response, the account was temporarily suspended; however as of May 2014 it is active. 125 No suspects were named, and there has been no news of further attacks; nonetheless, cybercrime is perceived to be a growing problem in Argentina.

125 Rodrigo Santos, “La Casa Rosada Cerró la Cuenta de Twitter Después de que Fue Hackeada” (Casa Rosada Closed Its Twitter Account After It Was Hacked), La Nación, August 21, 2013, http://www.lanacion.com.ar/1612482-la-casa-rosada-cerro-la-cuenta-de-twitter-despues-de-que-fue-hackeada
Armenia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Free</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td><em><em>TOTAL</em> (0-100)</em>*</td>
<td>29</td>
<td>28</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

<table>
<thead>
<tr>
<th>Population:</th>
<th>3 million</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Penetration 2013:</td>
<td>46 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 2014 Status:</td>
<td>Not Free</td>
</tr>
</tbody>
</table>

Key Developments: May 2013 – May 2014

- Access to the internet improved during the coverage period, with internet penetration increasing from 39 percent in 2012 to 46 percent by the end of 2013 (see Obstacles to Access).

- Improvements in the mobile market included the introduction of a mobile number portability (MNP) system in April 2014, allowing consumers to switch more easily between providers, and the licensing of a fourth mobile network provider, due to take effect in 2015 (see Obstacles to Access).

- On November 9, 2013, an amendment to the copyright law went into force that requires print publications, online media, and other websites to cite the original source of republished content, including the news outlet’s title and an active hyperlink to the original content where appropriate. Journalists and editors hope the new regulation will improve the quality of the media in Armenia (see Limits on Content).

- An online campaign surrounding pension reforms succeeded in generating a national policy change, eliminating the proposed requirement for mandatory pension contributions (see Limits on Content).
Introduction

The internet penetration rate in Armenia has continued improving over the past few years, accompanied by fewer restrictions on online content and increased efforts to make the communications regulatory body, the Georgian National Communications Commission (GNCC), more independent. Additionally, citizen groups and NGOs have made use of online communication tools to organize campaigns and promote policy changes in the country.

Obstacles to Access

Internet access in Armenia has increased, particularly in the past few years. According to the International Telecommunication Union, the internet penetration rate in Armenia stood at 46 percent in 2013, compared with 39 percent in 2012 and just 6.2 percent in 2008.1 Other estimates place the internet penetration rate somewhat higher: the Public Service Regulatory Commission estimated internet penetration in Armenia at 60.6 percent,2 while the Internet Society chapter in Armenia (ISoc Armenia) reported 56.9 percent,3 and the Caucasus Research Center placed the rate at 53 percent.4 These statistics generally vary due to differences in methodology used to calculate internet penetration rates.

The Armenian mobile phone penetration rate reached 112.4 percent in 2013, compared to 111.9 percent in 2012 and 48.4 percent in 2008.5 According to research conducted by Samvel Martirosyan, approximately 1.5 million mobile phones were connected to the internet as of February 2014, out of a total of 3.35 million mobile phone subscriptions.6 Technologies for wireless internet access in Armenia include 3G networks, WiMAX, and Wi-Fi. Access to mobile broadband is available throughout the majority of the country and is affordable for much of the population. Mobile broadband tariffs and limitations have become more affordable, and the networks more reliable, particularly for users in rural areas.7

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,8

---

7 Mobile operators providing mobile internet plans with guaranteed speed up to 50 Mbps for limited data volume (up to 50 Gb) and reduced speed (up to 512 Kbit/sec) after exceeding the limit.
8 This information was derived from reports published on several mobile operators' websites, including MTS (Mts.am), Beeline (Beeline.am), and Orange Armenia (Orangearmenia.am).
3G services are available to almost 100 percent of the population, covering 90 percent of the country (excluding mostly unpopulated mountainous regions).

In 2013, there were 58,000 fiber-optic network (FTTx) subscribers. The geographical range of these services mainly covers Yerevan and Abovyan. In 2012, the Russian-based company Rostelecom invested funds in “Fiber to the Home” technology in 11 towns across Armenia. In December 2013, it launched services in three additional towns: Abovyan, Ashtarak, and Gyumri. Rostelecom’s fiber network covers nearly 80 percent of Armenia’s territory and is connected with Iran and Georgia. Landline broadband access provided using ADSL technology is available in most cities and some villages.

Strong competition among the three primary mobile service providers and internet service providers in Armenia has resulted in fair market prices for both wireless and landline broadband services. ADSL connections with speeds of 3 Mbps are available for US$15 per month, optical landline connections with speeds of 12 Mbps are available for US$20 per month, and the price for a minimal volume (2 GB) package of mobile broadband service costs US$9 per month. Internet costs are relatively high when compared to the minimum salary in Armenia, which is US$125 per month. At the same time, considering that the average public utilities bill can vary from US$50 to US$100 in the summer and US$100 to US$300 in the winter, the cost of internet access is affordable for the majority of the population, whose average income is approximately US$380 per month. Additionally, the availability of free access points in the capital and almost all major cities makes internet services accessible for the majority of the urban population.

There have been some efforts to improve community access to the internet in the regions of Armenia; however, digital literacy remains somewhat low. On October 31, 2012, GNC-Alfa CJSC, in cooperation with the municipality of Yerevan, launched free public internet access in six public parks. In 2011, the municipality, in cooperation with several telecom operators and internet providers, enabled free Wi-Fi access at many public transport bus stations. Mobile operators also provide limited access in public spaces such as cafes and public transportation locations. Public access centers have now been launched in 11 cities, the centers of each of Armenia’s administrative districts (marzes). All schools in the regions of Armenia operate as public access points for communities. Moreover, every day from 2 PM (after school hours), access to social networks, such as Facebook and Odnoklassniki, are enabled for both schoolchildren and community representatives.

In practice, the Armenian government and the telecommunication regulatory authority, the Public Services Regulation Commission (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 such as Skype and Google Talk, and popular social networks such as Facebook, YouTube, and Odnoklassniki.

The continuous spread of broadband and high-speed internet access in the regions of Armenia, and the entrance of a new player in the mobile communications market, has increased the level of mar-

---


10 Armenian territorial divisions include 10 marzes and Yerevan, the capital of Armenia, which also has a status of marz.
ket competition, although the market for internet access in Armenia is still mostly concentrated in the capital city of Yerevan, which contains one third of the country's population.

There are currently three mobile telephone network operators in Armenia: Armentel/Beeline, whose owner is VimpelCom Ltd., one of the largest mobile network operators in Russia; VivaCell/MTS, a brand of MobileTeleSystems; and Orange Armenia. In 2013, Ucom Telecommunications Company was licensed as a fourth mobile network provider and is expected to launch on January 1, 2015. Under the terms of the Public Services Regulatory Commission's award, Ucom will deliver wireless broadband internet coverage in the capital Yerevan and its adjacent areas, as well as cover 80 percent of Armenia's provinces with mobile voice and mobile internet services in those areas. The license came into effect in November 2013 and will be valid until August 6, 2018.

On January 31, 2014, the Public Service Regulatory Commission adopted a measure allowing for customers to switch mobile operators while maintaining their current phone number. The Mobile Number Portability (MNP) system, which went into effect on April 1, 2014, allows subscribers to switch operators and keep their number free of charge, and has the potential to increase competition among mobile phone service providers by allowing customers to switch to better providers more freely.

The regulatory authorities in Armenia primarily focus on companies with significant market power. 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.

Armenian legislation requires that providers obtain a license for either the provision of internet services or the operation of a telecommunication network. 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{14}

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{15}

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.

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.\textsuperscript{16}

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.\textsuperscript{17} 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 Armenia lack independence due to the strong dependence of the commissioners’ career on political

\begin{flushleft}
\textsuperscript{16} The Law on Public Services Regulation Commission was adopted by the National Assembly of the Republic of Armenia on December 25, 2003.
\textsuperscript{17} Article 11 of the Law of the Republic of Armenia on Public Service Regulation Commission.
\end{flushleft}
leadership of the country. 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. 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.

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 of the independent regulatory authority, ISoc no longer plays as much of a regulating role, as most industry disputes are filed with the PSRC. Nevertheless, ISoc continues to maintain the registration of domain names, and despite the lack of formal dispute resolution policies (such as, for example, domain name disputes resolution procedures), it carries out the registry function effectively with minimal influence from government authorities or the regulator.

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 formally, members of the Armenian Internet Society are individuals, the organization’s board is composed of service providers’ 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.

Limitation on Content

The Armenian government does not consistently or pervasively block users’ access to content online. The only significant case of online blocking was reported in March 2008 during post-election events, immediately after clashes between an opposition rally and police resulted in at least eight people

---

18 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.


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-elections crisis, including the restrictions on access to internet resources. After the events of 2008, Armenian authorities have been 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 2012, Armenian users reported that they were not able to access Kavkazcenter.com, a Chechen-based website that reports on events in the Islamic world, particularly the ongoing conflict in the North Caucasus. The website was added to the Russian federal list of extremist materials by a court decision in September 2011. However, after Armenian bloggers and journalists reported on this issue, the telecom operator implemented measures to unblock the website within Armenia.

During 2014 there were reports of five other websites being blocked due to filtering in Russia by Roskomnadzor, the Russian telecommunications regulator. There was no explanation provided or information found about the reasons these websites were blocked in Armenia, and there are no apparent political reasons behind the blockings; ISPs explained the blocks as a technical problem and consistently took steps to remedy the issue after it was reported. Blocked websites usually contain no politically-sensitive information for Armenia or about Armenia, and usually websites that are blocked in Russia are available in Armenia.

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 and copyright-infringing materials. For example, in 2012 the Armenian police blocked the website Armgirls.am for disseminating pornographic content and for hosting bulletins of women working in the Armenian sex industry.

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 to their users.

---

21 “Special Mission to Armenia,” Council of Europe Commissioner for Human Rights, Reports on the number of people killed vary; according to the official report from the Council of Europe, eight people were killed. March 12-15, 2008, https://wcd.coe.int/ViewDoc.jsp?id=1265025.


24 The five blocked websites included Spigotmc.org (a forum website), www.35jobsworth.com (a jobs site), Electra.am (unknown), Rutor.org (a forum website), and Centrasia.ru (a news aggregating website). The website blockings were reported by blogger Samvel Martirosyan.


customers, provided that they had no prior knowledge of the content. Any decision of a law enforce-
ment 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 Hu-
man Rights; therefore, any such decision can also be challenged at the European Court of Human
Rights.

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 me-
dia outlets would restrict press freedom. The legislation was ultimately postponed for one year.

Currently, self-censorship is not a widespread practice in the online sphere. The Armenian gov-
ernment and the ruling political elite have avoided the application of any extralegal measures to
prevent political opponents or independent internet resources from publishing online content. How-
ever, 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 blog-
gers strongly resist self-censorship. Indeed, there is a wide diversity of opinion in social media, and
virtual battles between pro- and anti-government bloggers are often observed. A variety of inde-
pendent and opposition web resources provide Armenian internet audiences with politically non-bi-
ased, neutral, or oppositional opinions.

Two Armenian journalists—Kima Yeghiazaryan (of the newspaper Hayots Ashkharh) and Armen
Dulyan (from Shant TV)—were fired from their jobs for Facebook posts in March and June of 2013,
respectively. In both cases, the journalists expressed personal opinions that did not correspond with
the policy of the media outlet that they represented. Kima Yeghiazaryan criticized the government,
and Hayots Ashkarh is considered to be pro-governmental newspaper. Armen Dulyan criticized the
Russian television media and made parallels with Armenian media, characterizing the representatives
of both sides as “primitive.” Neither of the media outlets have a social media policy. Shant TV issued
a statement — incidentally, also published on Facebook — saying that future collaboration with
commentator Armen Dulyan could not be considered acceptable, since he displayed a “disrespectful


www.freedomhouse.org
attitude” toward the TV station. Both journalists’ employers either overtly or indirectly stated that their employee’s behavior on social media ran counter to their editorial policies. However, aside from these two incidents, the behavior of journalists on social media is generally not regulated in Armenian media.

An amendment to the law on Copyright and Related Rights took effect on November 9, 2013 and regulates the procedure and conditions for online news media to republish content. The legislation requires print media and websites to cite the original source when republishing excerpts of news and other content. The law also states that content providers must print the name of the original media outlet and, if the original content is from a website, include an active hyperlink. Compensation for damages is defined as 100 to 200 times the amount of the minimum salary (or approximately US$245 to US$490).

The Armenian government is very cautious about media freedom issues and tries to avoid direct pressure that may raise criticism from international organizations and local civil society activists. However, both the ruling political elite and the opposition party do have some influence over traditional and new media outlets. According to accounts from media professionals and civil society activists, most media outlets are either linked with a particular political party or periodically receive financial support from politicians, aside from two or three online media resources funded by foreign and international donor organizations. However, the extent to which this has a direct influence over the content of these media outlets cannot be easily assessed.

The financial model of Armenian online news resources is very similar to the model of the traditional print and broadcast media, in that the political elite may lend support to certain outlets through the channeling of advertising of government-loyal businesses. At the same time, websites such as the A1+ news editorial (A1plus.am) and Lragir Daily (Lragir.am), both of which publish articles that are critical of the government, are quite popular and have been able to survive economically. There are neither formal nor practical barriers to receiving domestic or foreign aid or advertisements, but foreign financial support is usually limited to modest grants, and foreign advertisers are usually not interested in the Armenian media market. A significant portion of advertising comes from mobile operators, banks, car dealers, and consumer electronics sellers.

The emergence of online media has caused a significant increase in journalistic activities in Armenia. Armenian media has traditionally been economically unsustainable due to the limited audience, high operational costs, and small advertising market. Even at the peak of media production in Armenia, daily newspapers usually published around 5,000 copies per day and few weekly outlets had more

34 Based on the interviews carried out with representative of Internex Armenia and the Center for Information Law and Policy.
Armenia

than 10,000 readers. The audience for television and radio was larger but still limited to the leading producers: five of the almost thirty television channels accounted for 76 percent of viewers. Early online news outlets such as A1+ enjoyed significant growth in the number of daily visitors during the first few years of production.

Armenian online news resources started growing from 2001 to 2005 when internet services became relatively affordable. However, the main increase in production of online content—particularly video and audio content—started in 2008 after the liberalization of the market and the decrease in the cost of broadband. Today, there are at least 30 leading online news outlets covering political, economic, and social issues. Since 2011, Armenia has seen the emergence of Armenian-language online television programs. Although online video news services are still underdeveloped and underused in Armenia, the public’s interest toward online video content is growing, and today at least three leading web resources—A1+ Online, Civilnet.am, and Azatutyun.am—offer on-demand video news and live-air reporting on major political and social events.

The majority of the population uses the internet mainly for social networking and as a cheaper alternative for voice and visual communication with relatives abroad. While those who use the internet in Armenia mainly visit news websites or social networks, given the overall low levels of daily internet use among the Armenian population, most Armenians still receive their news from television programs. Nevertheless, the population’s interest toward online news resources is growing, and the number of visitors to the leading news websites exceeds the number of the leading newspapers’ readers. Print copies of the leading Armenian newspapers—Aravot, Hraparak, and Iravunk—usually do not exceed 4,000 issues, whereas online news websites collect more than 700,000 unique visitors per day.

Armenian blogs and online communities are highly politicized and are likely to respond to most political events. During the last three years, social media—Facebook in particular—has been actively used for political and civil mobilization by the opposition and civil society activists. Besides Facebook, tools such as Livestream and Ustream are used by media outlets, NGOs, and online television stations (such as Civilnet.am, Azatutyun.am, and A1plus.am). These tools were used effectively during civic movements and protests against the rise in public transportation prices in July 2013 and during the ongoing movement against pension reforms, initiated by Dem.am in November 2013, which succeeded in changing the mandatory components in the legislation. NGOs have also used live-streaming tools to broadcast press conferences, discussions, debates, and other public events. For example, Levon Barseghyan, the director of the media NGO “Asparez,” live-streams sessions as a member of the local government’s city council, enabling the public to access information that was not previously available.

Another positive example of online mobilization is the iDitord (iObserver) project, a crowdsourced...
election monitoring project launched in advance of parliamentary elections in May 2012. The website received about 400 reports during the presidential elections of February 2013 and more than 400 reports from citizens, NGOs, and political parties during the Yerevan municipal elections of May 2013, mostly related to bribes, problems with the activities of local electoral commissions, violations of advertisement laws, and mistakes in electoral lists. The police and the Central Electoral Commission officially responded to some reports and claimed that others were not confirmed or were misinformed.

Violations of User Rights

Article 27 of the Constitution of the Republic of Armenia guarantees freedom of speech irrespective of the source, person, or place. The constitutional right to freedom of speech is universal and 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). One 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 toward 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 the 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 of 50-150 times the minimum salaries, 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 code to decriminalize defamation, including libel and insult, and introduced the concept of moral damage compensation for public defamation. The initial result was an increase in civil cases of def-

45 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).
amation, often with large fines as penalties. In November 2011, the Constitutional Court ruled that 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 a widely adopted legal practice 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 overthrowing of a legitimate government or constitutional order. As mentioned previously, the Armenian legal system is based on the principle of universality, meaning that laws are applicable online as they are offline. Therefore, all crimes conducted on the internet are prosecuted similarly to those that are conducted 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.

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.

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).

46 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

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.

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.

Cases of physical violence toward online journalists or other staff have not been recorded, though such instances have occurred with journalists from traditional media outlets.

DDoS attacks were not prevalent in Armenia until the start of the campaign period for the 2012 parliamentary elections. Blognews.am, an Armenian blogosphere aggregator, was attacked on the morning of April 20, 2012. Later, the iDitord.org website that covered election violations suffered from a DDoS attack. As a result, iDitord.org went down for several hours on election day; however, as a result of external DDoS mitigation services, the website was able to resume normal functioning after four hours of inaccessibility while attacks continued. The culprits of the DDoS attack are still unknown. During election day, iDitord was the only Armenian web site which came under DDoS attack. Additionally, during the presidential election on February 18, 2013, the opposition media website Galatv.am suffered from a DDoS attack. The staff at Haynews.am believed their website suffered from a DDoS attack on December 24, 2013 after they published a series of stories related to internal political life of Armenia, though the DDoS attack was not confirmed. The website was back online shortly thereafter.


Australia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td>Free</td>
<td></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>10</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>17</td>
<td>17</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 23.1 million
Internet Penetration 2013: 83 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Free

Key Developments: May 2013 – May 2014

- Broadband access continued to expand for online users as the National Broadband Network reached more rural and remote communities (see **Obstacles to Access**).
- Concerns over ISP filtering practices continued in response to the government’s consideration of a graduated response scheme and the blocking of piracy websites (see **Limits on Content**).
- Revelations regarding global surveillance and the retention of communications data by intelligence agencies, and legislative proposals in the Australian parliament that could increase government surveillance, raised concerns regarding internet users’ right to privacy and freedom of expression (see **Violations of User Rights**).
Introduction

Australia enjoys affordable, high-quality access to the internet and other digital media, and this access has continued to expand over the past few years with the rollout of the National Broadband Network. However, recent amendments to surveillance legislation and proposals to implement censorship through directives to internet service providers (ISPs) have raised concerns about privacy and freedom of expression.1

Additionally, in late 2012 Australia acceded to the Council of Europe's Convention on Cybercrime, which brought into effect a number of obligations for ISPs to monitor, preserve, and store user data. However, Australia's legislation goes beyond the requirements set out in the Convention by requiring longer retention timelines for foreign preservation notices, and requiring ISPs to cooperate with any serious crime being investigated in Australia or overseas.

Obstacles to Access

Australia had an internet penetration rate of approximately 83 percent as of December 2013, according to the International Telecommunication Union.2 From 2012 to 2013, there was a 2 percent increase in internet subscriptions, with 12.4 million internet subscribers in Australia (excluding internet connections enabled through mobile phone handsets) and 19.6 million mobile handset subscribers.3 The internet penetration rate is expected to steadily increase over the next five years with the implementation of the National Broadband Network (NBN), which includes expanded wireless and satellite services in rural communities. Although internet access is widely available in locations such as libraries, educational institutions, and internet cafes, 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+, wireless, cable, satellite, and dial-up.5 Wireless systems can reach 99 percent of the population, while satellite capabilities are able to reach 100 percent.6 As of December 2013, over 98 percent of internet connections were broadband, while the number of dial-up connections has declined to 2 percent.7 Once implemented, the NBN

---

7 Ibid.
Australia

will 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 of 256 Kbps or greater. While there are still parts of Australia experiencing slower broadband speeds (1.5 Mbps to 8 Mbps), there has been a steady increase since 2012 in connections with faster speeds.\(^9\) Under the revised NBN roll-out, it is expected that two-thirds of Australian’s will have download speeds of nearly 100 Mbps by 2019.\(^10\)

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.

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.\(^11\) Of those with internet access, 85 percent access the internet through broadband connections.\(^12\) The overall mobile phone penetration rate in Aboriginal communities is unknown.

According to the International Telecommunication Union, Australia had a mobile phone penetration rate of 108.6 percent, or 24.9 million subscriptions, in 2013.\(^13\) Third generation (3G) mobile services are the driving force behind the recent growth, with 25.8 million mobile subscriptions operating in 2013.\(^14\)

Internet access is affordable for most Australians. The government subsidizes satellite phones and internet connections for individuals and small businesses in remote and rural areas, where internet affordability is not comparable to that in metropolitan areas.\(^15\) Major ISPs such as Telstra also continue to offer financial assistance for internet connections to low-income families.\(^16\)

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.17

Like most other industrialized nations, Australia hosts a competitive market for internet access, with 76 providers as of December 2013, nine of which are very large ISPs (over 100,000 subscribers), another 19 large ISPs (with 10,001 to 100,000 subscribers), and 48 medium ISPs (with 1,001 to 10,000 subscribers).18 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.19 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).20 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.21 The industry's involvement consists of developing industry standards and codes of practice.22

The ACMA is the primary regulator for the internet and mobile telephony.23 Its oversight is generally viewed as fair and independent, though there are some transparency concerns with regard to the classification of content. Small businesses and residential customers may file complaints about internet, telephone, and mobile-phone services with the TIO,24 which operates as a free and independent dispute-resolution service.

Limits on Content

Australian law does not currently provide for mandatory blocking or filtering of websites, blogs, chat rooms, or platforms for peer-to-peer file sharing. 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

---

17 Telstra, page 19.
to the Telecommunications Industry Ombudsman. 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.

It has meanwhile been reported in the news that the federal cabinet is considering two proposals that address piracy and the illegal downloading of content protected by intellectual property rights. The first proposal will require ISPs to issue warnings to users who repeatedly download illegal content (predominantly songs, movies, and TV shows) within a “graduated response scheme” where repeat offenders may have their internet accounts temporarily suspended. The second proposal will force ISPs to block file-sharing sites such as Pirate Bay. However, neither initiative has been formalized into a proposal or bill at this point.

As of May 2014, parliament is considering a bill that would allow automated classification tools to be used in lieu of or to aid the classification of publications, films, and computer games. The bill is mainly procedural at this point. There is no information as to the type or nature of “classification tools” that would be used, or how they would change the workflow and human input into the classification process. In the bill’s current wording, the minister of communications would have wide discretion to approve any tool. The bill has been criticized for not requiring transparency in the selection of classification tools, and for not having a sunset clause that would require reviewing the use of tools after a trial period.

There are no examples of online content manipulation by the government or partisan interest groups. Journalists, commentators, and ordinary 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

---

25  Ibid.
29  Classification (Publications, Films and Computer Games) Amendment (Classification Tools and Other Measures) Bill 2014 (Cth).
users (see “Violations of User Rights”). 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.\(^{32}\)

There remains a lack of adequate legislative protection for the confidentiality of journalist’s sources.\(^{33}\) However, on a positive note, on January 15, 2014, the Commonwealth Public Interest Disclosure Act came into force providing protection to whistleblowers. Previously, whistleblowing protection was only for those disclosing information from State government initiatives; the protection now extends to the Commonwealth government.

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 both as sources of information and as tools for mobilization. One interesting development has been the announcement by the new attorney general, George Brandis of his desire to repeal S 18C of the Racial Discrimination Act 1975 (Cth). Section 18C, otherwise known as the hate speech provision, currently makes it unlawful to commit an act (by any medium of communication) that is likely to offend, insult, humiliate or intimidate another party based on race, colour, or national or ethnic origin of another party. The announcement was met with strong public backlash from organizations and entities dedicated to combating racism online.\(^{34}\) Ultimately the Abbott administration announced that it would not move forward with the proposal to remove section 18C of the legislation.\(^{35}\)

Advanced 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.\(^{36}\)

### Violations of User Rights

While online 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. Over the past year, 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

---

\(^{32}\) Nick Title, “Open Justice – Contempt of Court” (paper presentation, Media Law Conference Proceedings, Faculty of Law, The University of Melbourne, February 2013).


Australia

taken few steps to remedy these concerns, and 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.

Australians’ rights to access internet 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. 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).

The Australian press, however, has consistently expressed concerns about a “culture of secrecy” that continues to inhibit reporting. A 2007 report commissioned by Australia’s Right to Know (ARTK), a coalition of media companies formed to examine free press issues, found that there were over 350 pieces of legislation containing “secrecy” provisions to restrict media publications. As revealed in the Media Entertainment & Arts Alliance report on press freedom in Australia, secrecy and surveillance remain a critical issue.

The Anti-Terrorism Act 2005 (Cth) revived laws against sedition and unlawful association. The unlawful association provisions have been used widely since their enactment to ban several organizations perceived to be potentially dangerous in terms of their links to violent acts. The sedition provisions, however, have not been used. Further, insults against government institutions or officials would not fall within the sedition provisions.

Australian defamation law has been interpreted liberally and is governed by legislation passed by the states as well as common law principles. 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. Court costs and

42 Ibid.
44 Moss, 42.
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.46

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.

In the recent case of Mickle v Farley,47 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 student’s father was also a teacher at the school. The father left his position due to health reasons but the student grudgingly blamed the new teacher, Ms. Mickle, who took his father’s position. The comments greatly distressed Ms. Mickle, forcing her to take sick leave shortly after the allegedly hateful comments were posted to social media. The case is 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.48 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.”49

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, 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.50 The sentence was appealed and the court commuted the original sentence in favor of a suspended sentence.

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 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.51

48 A 2011 case involving writer and TV personality Marieke Hardy reached a legal settlement in 2012.
49 Ibid. Line 21.
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. The collection and monitoring of the content of a 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).\(^{52}\) 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.\(^{53}\) Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.\(^{54}\) The TIAA and TA expressly 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.\(^{55}\)

On August 22, 2012, the Australian Senate passed the Cybercrime Legislation Amendment Bill, allowing Australia to accede to the Council of Europe Convention on Cybercrime.\(^{56}\) Unlike the legislation of many other countries that have already ratified the convention, Australia’s legislation goes beyond the treaty’s terms by calling for greater monitoring of all internet communications by ISPs. Under the Convention, an ISP is only required to monitor, intercept, and retain data when presented with a warrant, and only in conjunction with an active and ongoing criminal investigation restricted to the areas in the Convention: child pornography, online copyright (intellectual property), online fraud and forgery, and computer offenses. The new Australian legislation compels ISP cooperation for any serious crime being investigated in Australia or overseas; it is not limited to the crimes set out in the Convention.

The Convention also requires expeditious preservation of data by the person in possession or control of data, which means ISPs will often be the ones called upon to store data. Articles 16 and 17 of the Convention state that ISPs can be compelled to preserve internet traffic data logs for a maximum period of 90 days, whereas the Australian legislation mandates that ISPs store data for 180 days for foreign preservation notices. However, the Convention does not compel ISPs to monitor stored communications, only traffic data. In the case of an active criminal investigation, the Convention obligates an ISP to preserve the data that is already stored but would otherwise be deleted. This could include preservation of what IP addresses connect to and from other IP addresses, or what phone numbers connect to a Voice over Internet Protocol (VoIP) number. This may also include information about what types of protocols a customer uses, the size and use of packets, and so forth. Data preservation remains a controversial point but most notably in relation to the obligation to provide mutual assistance to a foreign entity.

In July 2012, the Commonwealth Attorney-General’s Department released a discussion paper titled


“Equipping Australia against emerging and evolving threats.” Under the proposal, Australian ISPs would be required to monitor, collect, and store information pertaining to all users’ communications, including storing communications, for a period of two years. This activity would be done without a warrant and enforced against all users regardless of whether there is a criminal investigation. The 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 strike down 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. This compulsory data retention policy, if enacted, could become a significant threat to internet freedom in Australia. The proposal is not yet official policy in Australia, nor has it evolved to a bill. At this point in time it remains a proposal only.

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.”

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 already come 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. Cyberattacks and hacking incidents remain a common and growing concern in Australia. Several 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

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>13</td>
<td>14</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>22</td>
<td>24</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>52</td>
<td>55</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 9.4 million
Internet Penetration 2013: 59 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Internet cafes were reportedly forced to temporarily shut down in the Nakhchivan region as part of a ban on gatherings ahead of the presidential election (see Obstacles to Access).

- An increasing number of journalists and activists who are active online were given harsh prison sentences on trumped-up charges (see Violations of User Rights).

- In May 2013, amid a growing crackdown on press and online freedoms ahead of the presidential election, the parliament passed amendments to the criminal code that extended criminal penalties for defamation to online content (see Violations of User Rights).
Introduction

During the opening remarks at the third International Humanitarian Forum hosted in Baku on October 31, 2013, President Aliyev spoke proudly of how far Azerbaijan has come in developing internet technologies.\(^1\) In his speech he referred to the “totally free” environment of the internet in Azerbaijan with a growing penetration rate of 70 percent, assuring his audience that “any intervention is out of [the] question here.”\(^2\)

And yet according to the local advocates, the reverse trend is under way, with an increase in restrictions on online activities witnessed ahead of the presidential elections. On October 9, just a few weeks before the humanitarian forum, Azerbaijani voters went to the polls to elect their next president. In what was yet another in a series of contested elections, Ilham Aliyev won the overwhelming majority of the votes with 84.6 percent, with international observers noting a range of violations including ballot box stuffing and limitations to freedom of expression, freedom of assembly, and freedom of association in the run-up to the election.\(^3\) In particular, on May 14, 2013, the authorities extended criminal defamation provisions to online content.\(^4\) According to the new amendments to the criminal code, which were signed into law in June by President Aliyev, penalties could include fines as high as AZN 1,000 (approximately US$1,300), community service, corrective labor and prison sentences for up to three years in certain cases.

The Azerbaijani government continues to practice minimal filtering and online censorship; however, in contrast to the government-disseminated image of a free and open internet, in 2013 and 2014 the government imposed harsher sentences on bloggers and online activists, with offline intimidation also increasing. Reports of internet cafes shut down in the autonomous region of Nakhchivan ahead of the elections to avoid any protests, were also disturbing. While the local officials denied any such instances,\(^5\) there have been previous attempts to close down internet cafes in Garachuxur and Guneshli districts of Baku and in the Ismayilli region during the January 2013 protests. The crackdown on internet cafes in Nakhchivan began on August 23, 2013, less than two months prior to the presidential elections in Azerbaijan.

Despite these limitations, the internet remains a platform for information-sharing and a medium for alternative voices and popular political dissent, particularly as the government maintains tight control over traditional media outlets.

---

Obstacles to Access

There have been several improvements to the internet infrastructure in Azerbaijan over the past year, including plans to introduce a countrywide broadband connection, a decrease in internet costs, and a growing internet penetration rate. Despite these developments, the overall quality of internet access remains low, especially outside the capital and larger towns where dial-up is still the most common method of online access. In addition, the state security forces are free to visit internet service providers (ISPs) whenever they like. The Ministry of Communication and Information Technologies 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.6

Based on the most recent report on the percentage of individuals using the internet released by the International Telecommunication Union (ITU), by the end of 2013 Azerbaijan had an internet penetration rate of 58.7 percent, compared to 54.2 percent in 2012 and 17 percent in 2008.7 Mobile phone subscriptions reached a penetration rate of 107.6 in 2013,8 while rates for mobile broadband penetration were at 33.3 percent.9 However, statistics for internet penetration rates vary according to the source. For example, according to official statistics referred to by government officials, internet penetration in Azerbaijan reached 70 percent in the last two years.10 This number includes mobile internet users as well as anyone who has accessed the internet, including one-time users.11 Another statistic from the Delta Telecom technical director, Raed Alakbarli, holds Azerbaijan’s internet penetration rate at only 44.4 percent as of May 2014.12

Access to the internet in rural areas remains difficult. Although there are a variety of ISPs in the country, few have the infrastructural capacity to provide access to rural areas, leaving many residents to access the internet through dial-up or mobile connections. The quality of access is also below average, especially anywhere outside the main cities. In September 2013,13 the government announced an ambitious plan worth US$131 million to build the infrastructure for countrywide broadband internet and to cover all areas of the country with high-speed internet access by 2017. The initiative seems to have stalled, however, as the selection of technologies for implementation of

---

6 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. “Searching for Freedom: Online Expression in Azerbaijan,” The Expression Online Initiative, November 2012, http://www.irfs.org/wp-content/uploads/2012/12/Report_EO_1.pdf
10 ‘Number of Internet users to be increased to 85% in Azerbaijan’, December 25, 2013, apa.az, http://en.apa.az/xeper_number_of_internet_users_to_be_increased_204854.html
12 “Azerbaijan has over 4 billion unused Internet resources”, abc.az, May 19, 2014, http://abc.az/eng/interview/96.html
Azerbaijan

the project still continues. In addition to infrastructural obstacles, there is a gender gap in internet access rates as women across the country, particularly in the rural regions, face a number of barriers to access, from cultural norms disapproving of women using the internet to a lack of education and access to technology.

In order to make internet service available countrywide at lower costs, on December 24, 2013, the Ministry of Communications and Information Technologies (MCIT) announced their plan to reduce tariffs on internet services. While the overall price charged by the providers has increased, the plan suggests further cost reductions. However, any cost reductions depend on ISPs ensuring quality delivery of content. According to Ramazan Valiyev, the CEO of the primary Azerbaijani provider Delta Telecom, the only obstacle to improving internet access is the need to replace all existing copper cable infrastructure with fiber-optic lines. With new fiber-optic cables, the connection speed can reach a minimum of 10 Mbps rather than the current 2-3 Mbps. According to Akamai, the average connection speed in 2013 was 2.85 Mbps. The comparison with previous years shows very little growth, thus calling into question government statements on the growth and improvement of the ICT sector.

Based on official data, the cost of internet access has dropped over the past five years. Currently, according to the minister of ICT, the cost for internet access is about 2 percent of the average monthly wage. However, according the Azerbaijan Internet Forum, internet access remains an expensive commodity for many Azerbaijanis, especially in comparison with neighboring countries. The most recent indicators provided by the Azerbaijan Internet Forum indicate an average cost of US$25-75 for an unlimited 4-8 Mbps ADSL connection.

The growth in mobile phone usage continued over the past year. Azercell remained the leading mobile service provider, although its overall market share fell from 50 percent to 43 percent. Azerfon and Bakcell, the other two largest mobile operators, maintained market shares of 24 percent and 33 percent, respectively. In August 2013, both Azerfon and Bakcell launched a Mobile Number Portability (MNP) service. This service allows mobile operator users to switch from one network to another without having to lose their numbers, thus potentially increasing competition among providers.

18 https://www.facebook.com/multimediaosman/posts/349178915221658
Introduction of 3G services and changes in mobile phone data packages provided by the phone companies lowered the average costs of mobile internet from AZN 40.50 (approximately US$50) in 2011 to AZN 7.75 (approximately US$10) in 2012. The average connection speed improved significantly in 2011, increasing from 3.48 Mbps to 7.05 Mbps. According to Reporters Without Borders, 31 percent of mobile subscribers access the internet on their phones. In addition, bureaucratic obstacles have led to delays in the introduction of a 4G LTE network. The only provider of 4G LTE in Azerbaijan is Azercell, but access is limited to certain areas.

In the run-up to the presidential elections, several internet cafes were reportedly closed down by the Azerbaijani authorities in Azerbaijan’s Autonomous Republic of Nakhchivan. The Institute for Reporters’ Freedom and Safety (IRFS) reported that beginning on August 23, internet cafes were subject to closure. According to the report, internet cafe owners said the Ministry of Communications and Information Technology of Nakhchivan issued these orders in an attempt to curb online dissent ahead of the elections. In a region with a poor human rights record, political liberties are highly restricted, 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.

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 internet providers including three state-owned providers: AzTelekomnet (Azertelecom), BakInternet and Azdatakom. Delta Telecom is also the owner and operator of the largest fiber-optic backbone in the country. 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 MCIT and whose shareholders include Azerfon, with links to the president’s daughters. 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 for cheaper phone calls.

Since 2000, ISPs are no longer required to obtain a license. While the MCIT reports that there are over 40 ISPs in the country, Net Index categorizes only 20 of these as “main” ISPs. Delta Telecom and Azertelecom are two private companies that provide access to the international internet.

---

Azerbaijan

Apart from holding a monopoly over the sale of the “.az” domain, the Ministry of Information and Communication Technologies also performs the basic regulatory functions pursuant to the 2005 Law on Telecommunications. On February 14, 2013, the Azerbaijani Press Council established a commission under the government-controlled National Television and Radio Council to handle citizens’ complaints about ethical violations online, hacking attacks on web pages, and other issues related to online media.\(^{32}\) As of May 2014, however, the Press Council has filed no such reports and has raised no concerns over the state of media freedom in Azerbaijan. In fact, on May 2, 2013, the Press Council came together with the National Television and Radio Broadcasting Council and the Foundation of State Support for the Development of Mass Media under the President of Azerbaijan to celebrate the current state of “free and fair online and offline media” in Azerbaijan.\(^{33}\)

**Limits on Content**

There is no systematic or widespread blocking or filtering of websites or social networks, as the government relies mainly on other means of control through intimidation and arrest of users. In the past, some sites experienced temporary access issues, especially during protests in specific areas of the country. The image-uploading site Imgur was blocked in January 2013 after hackers from Anonymous obtained and posted 1.7 GB worth of documents from the Special State Protection Service of Azerbaijan;\(^{34}\) as of May 2014 the site remains inaccessible.\(^{35}\) Sporadic filtering has also become a problem for opposition websites from the Azerbaijani diaspora, such as Azdiaspora.org. Other websites, such as Tinsobhbeti.com, a website with satirical articles, caricatures, and videos about government and government corruption, and Susmayaq.biz, a website for public campaigning, were both shut down in 2011 and 2007, respectively.\(^{36}\)

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/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.\(^{37}\) Additionally,

---


There is still no established process through which affected entities can appeal in cases where opposition websites or other materials have been blocked. Decisions to block online content are not transparent, and when users try to access blocked websites (such as Imgur) 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. Libel and defamation are the most commonly used charges, as they remain a criminal offense.

As journalists, activists, and those critical of the government have increasingly turned to the internet to express their views, the Azerbaijani authorities have amplified their efforts to clamp down on online activities and stifle opposition voices through tactics such as internet cafe raids, netizen arrests, and other extralegal intimidation (see Violations of User Rights). Some state universities warn students that they will encounter problems, including threats of bad grades or detention, if they participate in online political activism. Students are instead urged to be very active in defending the government and its positions in their posts and comments on Facebook and other social media. These efforts have had a chilling effect on internet users who may be practicing self-censorship out of fear of government reprisals, although the extent of self-censorship online is not as widespread as in the traditional media.

To further discourage Azerbaijani youth from using the internet and social networks, members of the government have implemented a number of different tactics in the past few years. Early in 2011, the country’s chief psychiatrist, Garay Geraybeyli, described “people who prefer communication on social networks [as] having mental problems.”\footnote{“Social network users have ‘mental problems’,” Trend.az, March 7, 2011, http://en.trend.az/news/society/1841409.html.} Not surprisingly, the statement came four days prior to the March 11 Great People’s Day in Azerbaijan, an online initiative organized through Facebook calling people to join in the struggle for freedom and democracy in Azerbaijan in a civil way, without provocations, in villages and cities across the country.\footnote{Facebook page for “March 11, Great People’s Day in Azerbaijan” public event https://www.facebook.com/events/192209267477787/} In another attempt, a television program featured stories of “severe Facebook trauma” and “illness” as a result of use of social media. On April 2, 2013, an article published online on Xezerxeber.com described social networks as “cholera of the 21st century.” The paper claims that social networks create jealousy among its users.\footnote{“Social networks create jealousy”, Xezerzeber.com, April 2, 2013, http://xezerxeber.com/XeberOxu.aspx?id=55717#UV33UxlhOaI [in Azerbaijani]} On May 6, 2013, Azerbaijani Communication and IT Minister Ali Abbasov expressed his concern with social networks, characterizing them as platforms for insult and claiming that five to ten percent of divorces are caused by the negative impact of the internet.\footnote{“Minister: Illegal behavior on Internet needs regulating in Azerbaijan,” May 6, 2013, En.trend.az, http://en.trend.az/capital/business/2147219.html} In another attempt to discourage the use of internet and social networks, one local paper wrote that using the internet creates a harmful habit of internet dependency. The article describes the results of some unknown research, according to which one out of every 10 internet users is bound to acquire the “harmful” habit.\footnote{“Ciddi təhlükə yaradan internet asılılığı,” April 24, 2014, Azadxeber.net, http://www.azadxeber.net/ciddi-thlk-yaradan-internet-asll_h26577.html.}
Azerbaijan

Government-friendly online media outlets are the main beneficiaries of the advertising market. As is the case in the traditional media sphere, state-owned and private companies tend to refrain from advertising their products in independent or opposition online media. Furthermore, independent or opposition media outlets face additional pressure from the authorities in the form of fines and lawsuits.

The opposition newspaper Azadliq has been subject to fines and harassment from the authorities over the past few years, and the crackdown on the media outlet appears to be intensifying. In September 2013, the newspaper suffered a lawsuit after it reprinted content from a Facebook post. The subject of the post considered the content to be libelous, and sued the newspaper for AZN 50,000 (US$63,000) after they reprinted it.45

On May 13, 2013, the founder and editor of the online newspaper Veteninfo.az, Nahid Janbakhisli, reported that a lawsuit had been filed against him by the head of the Imishli District Executive Power, Vilyam Hajiyev. On April 11, Janbakhisli had published an article titled, "Businessman arrested because of Vilmay Hajiyev," on the publication’s website. In the lawsuit, Hajiyev demanded AZN 100,000 (approximately US$127,405) for “humiliation of his honor and dignity and retraction of the false information damaging his business reputation."46 On June 28, 2013, following two court hearings, the presiding judge rejected Hajiyev’s claims.

Blogging in Azerbaijan began gaining popularity in 2007. With the introduction of Azerbaijani-language blogging platforms, active bloggers writing in the native language provide an alternative source of information on many subjects that are ignored or distorted by traditional media. There are over 150,000 bloggers and microblog-users in Azerbaijan.47 Most of these blogs are written in the Azerbaijani language, and only about 1,000 blogs are written in English, Russian, or other languages. Many bloggers, such as Ali Novruzov, Emin Milli, Emil Bagirov, Etibar Salmanli, Arzu Geybullayeva, and Zaur Gurbanly, are well known for their independent views, and an estimated 50,000 to 70,000 users read blogs online. Additionally, according to the head of the Press Council in Azerbaijan, more than 10 internet radio stations and television channels operate within the country, and over 100,000 users watch television online. There are also more than 40 online news websites.48

Access to social media applications such as Facebook and Twitter is unrestricted, and such sites are increasingly used to disseminate content critical of the government. Facebook, in particular, has become a key source of information on rallies, protests, and social issues such as housing demolitions. The number of registered Facebook users grew from approximately 700,000 in December 2011 to over 1,000,000 users in 2013.49 As of October 2013, 1,250,000 Azerbaijani have

---

47 “Bloggers are passive: in Azerbaijan blog users are not active,” Video, YurdTV, March 5, 2013, http://yurd.tv/yurdxedber/20130302085717673.html [in Azerbaijani]
Azerbaijan

an existing account on Facebook. The majority of Facebook users in Azerbaijan are youth, at 74 percent.50

Youth activists, organizations, and political movements are widely represented in social media, providing information, organizing activities and events, and arranging protests via the internet. Inspired by the Arab Spring uprisings in early 2011, young activists in Azerbaijan continue to use social media to organize demonstrations against the government’s authoritarian rule, calling for democratic reforms and an end to pervasive government corruption.51

In September 2012, Elshad Abdullayev, the former director of the now-defunct Azerbaijan International University, began uploading videos to YouTube that exposed corruption on the part of Gular Ahmedova, a high-ranking figure and member of the ruling party.52 The first video footage of this scandal, referred to as “GularGate,” exposed Ahmadova attempting to sell a parliamentary seat to Abdullayev for AZN 500,000 (approximately US$636,000). Ahmadova was stripped of her parliamentary mandate, expelled from the ruling party, and placed under house arrest. On February 13, 2013, the Prosecutor General’s Office announced that Ahmadova had been charged under Article 178.3.2 for fraud (embezzlement) and Article 307.2 for concealment of a serious crime without agreement.53 In what was described by human rights advocates in Azerbaijan as a deliberate turn of events, Ahmadova was released by the decision of the Baku Court of Appeals on May 5, 2014. The court replaced the original sentence with a three year suspended sentence.54

A series of protests were organized starting in January 2013, including at least one through the Facebook page that translates as “End Soldiers’ Deaths.”55 Held in Baku, this unsanctioned rally was organized to protest the death of military conscript Ceyhun Qubadov. According to local reports, hundreds to thousands of people gathered at the Fountain Square holding signs with slogans about the mistreatment of military conscripts in Azerbaijan. While there were no arrests, police issued fines to 29 protestors. Facebook was quickly put to use once again to organize an online fundraiser through the “Five Cents” campaign. The campaign managed to raise AZN 12,500 (approximately US$16,000) from 7,000 people over a two week period. Thirteen activists paid their fines from this amount, while the rest was donated to the family of the conscript. Those who refused to pay their fines began a civil disobedience campaign.56

Most likely in response to this fundraising campaign, a new sub-article was added to the Code on Administrative Offenses in February 2013, which requires anyone providing or donating monetary assistance of more than AZN 200 (approximately US$255) to political parties, civil society

50 “False Freedom: Netfreedom in Azerbaijan, after the 7th Internet Governance Forum,” October 2013
52 As of February 2013, eight videos have been released.
55 https://www.facebook.com/Esgerolumerine.son?ref=ts&fref=ts
organizations, or international NGOs to register the donation with the Ministry of Justice. Those who fail to do so will receive fines ranging from AZN 250 to AZN 7,000 (approximately US$300-9,000). Institutions that accept these donations are also subject to fines, ranging from a minimum of AZN 1,000 to a maximum of AZN 10,000 (approximately US$1,300-13,000).

Violations of User Rights

The Azerbaijan government continues to arrest and harass online users, particularly young activists and journalists who post information and opinions critical of the government. In May 2013, the parliament passed amendments to the criminal code that extended existing criminal penalties for defamation to the online sphere, and began to prosecute individuals under this law for content posted on social media sites. The government increased its crackdown on civil society by arresting more activists and inflicting harsher sentences, including the sentencing of eight youth activists to prison terms ranging from six to eight years.

Articles 47 and 50 of the constitution guarantee freedom of speech, provide the right to distribute information, and prohibit state censorship of the mass media. In addition, as a signatory of the International Covenant on Civil and Political Rights (ICCPR), Azerbaijan is obliged to respect the right to freedom of expression. In practice, however, the authorities aggressively use various forms of legislation to stifle free speech in print and broadcast media. The judiciary lacks independence and is largely subservient to the executive branch.

Libel is the most common criminal offense 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.

An alternative bill—the Draft Law on Protection from Defamation—was designed in cooperation

---

59 Eight activists were sentenced in this court case: seven members of the youth movement NIDA, and one member involved in another youth movement.
60 The constitution is available in English at http://en.president.az/azerbaijan/constitution
Azerbaijan

with civil society institutions and the OSCE office in Baku in 2012. However, the original text was not taken into account and was instead watered down behind closed-door discussions among government actors. Provisions were removed from the bill that would have repealed criminal liability for defamation and reduced the maximum monetary penalties to match that of other civil violations. By leaving these clauses out, the authorities maintained the threats to freedom of expression inherent in the legislation.

Over the past year, more bloggers, human rights defenders, and activists have been detained or prosecuted for their online activities. On May 6, 2014, a court sentenced eight activists, including seven members of the NIDA civic movement, to prison sentences varying from six to eight years. Originally the group faced charges ranging from drug possession to illegal possession of explosives; on September 12, 2013, they were also charged with planning to organize acts of public disorder and intending to use Molotov cocktails. Ilkin Rustamzade, a 21-year-old activist and member of the Free Youth movement, was tried along with the group. Rustamzade was initially charged with "hooliganism" for allegedly filming and uploading a version of the global internet meme "Harlem Shake" to YouTube, though he denies any involvement in the video. He was also later charged with using Facebook to assist the NIDA activists in organizing the March 10, 2013 protests. Rustamzade was convicted and sentenced to eight years in prison. The other activists on trial were also convicted; during their hearing, the presiding judges provided their Facebook posts and online correspondence as evidence of their actions.

The prison sentences that individuals have received over the past year have signaled a substantial crackdown on freedom of expression by the authorities. Other activists and journalists arrested or sentenced during the coverage period for their online activities include:

- Nijat Aliyev, editor-in-chief of the news website Azadxeber.net, was arrested in May 2012 on charges of drug possession and was later given additional charges of unlicensed distribution of religious literature, making public calls to overthrow the constitutional regime, and incitement of ethnic hatred. On December 9, 2013, he was sentenced to 10 years in prison. The editor-in-chief denied the charges, saying it was Azadxeber’s reporting on the government’s religion policies that prompted his arrest.

- Rashad Ramazanov (Rashad Hagigat Agaaddin), a blogger and Facebook user critical of the government and some of its high-ranking officials, was detained near a metro station on May 9, 2013 and taken to the Department for Combating Organized Crime. Ramazanov was charged with drug trafficking after police reportedly found nine grams of heroin in his pocket; however, Ramazanov rejected the charges and insisted that the drugs were planted on him. Furthermore, although Ramazanov was legally supposed to be transferred to an Investigative Detention Center within 24 hours of his arrest, he was held at the organized crime unit for 11 days. When his lawyer was finally allowed to see him, he reported that

---

Ramazanov had suffered serious head injuries while in detention. On November 13, Ramazanov was sentenced to nine years in prison for drug trafficking under article 234.4.3 of the criminal code.

- Hilal Mammadov, a human rights defender and editor of the newspaper Tolishi Sado, was arrested on June 21, 2012 for illegal drug possession, treason, and incitement to national, racial, social and religious hatred and hostility. Mammadov was arrested after he shared a video on YouTube called “Ti kto takoy, davay dosvidaniy!” (Who are you? See you, goodbye!). In the video, two brothers perform a meykhana—a literary and folk rap tradition that involves improvising on a particular topic. The main jingle, which is in Russian, was first introduced by a Russian Car Owners Federation official who posted on Twitter: “Putin, who are you? See you, goodbye.” The jingle, which was transformed into just “Who are you? See you, goodbye,” was later used by other groups in Russia, Georgia, and Armenia in political contexts. The video of the two brothers received many clicks and grew in popularity due to the nature of verses. Shortly after, Mammadov posted a comment under the video where he wrote that the video had made Azerbaijan more popular than the government had been able to despite all the money spent on the Eurovision song contest. He was arrested following this comment. On September 27, 2013, Mammadov was sentenced to five years in prison.

- On August 2, a district court in Baku ordered the detainment of Sardar Alibeyli, editor-in-chief of the independent online news outlet P.S. Nota, for two months pending an investigation based on hooliganism charges. Alibeyli has also faced trumped-up charges against him in the past. In April 2007, Alibeyli was convicted and sentenced to 18 months of corrective labor for defaming Minister of Interior Ramil Usubov. Two years later, in July 2009, he spent three months behind bars on criminal defamation charges. Alibeyli wrote critical pieces about President Aliyev and his administration, in addition to posting commentaries by exiled politicians accusing the president of corruption, human rights abuses, and authoritarianism. Prior to his arrest in August, he shared a collage on Facebook depicting Aliyev in handcuffs. In November, Alibeyli was convicted of hooliganism and sentenced to four years in prison.

- Taleh Bagirov (Bagirzade), a religious scholar and activist, was arrested on March 31, 2013. Bagirov is known to be critical of the Azerbaijani government in his sermons (some of his sermons are available on YouTube. His final video received over 36,000 hits). He was charged with illegal drug possession with intention to sell under Article 234.1 of the Azerbaijani criminal code. According to Bagirov’s lawyer, Anar Gasimli, he was unable to see his client for a week. When Gasimli finally did see Bagirov, the activist told him he was abused and beaten while in custody. During their meeting, the defendant was heavily bruised and unable to move three of his fingers. Requests for immediate medical examination were never met. In March, Bagirov was sentenced to two months in pre-

71 Haci Taleh Bagirzade arrested following this speech, March 24, 2013, https://www.youtube.com/watch?v=KUmEb7O43-A
trial detention. His sentence was extended on May 24. In November 2013, Bagirov was convicted of drug possession and sentenced to two years in a strict regime prison.\footnote{Felix Corley, ‘Azerbaijan: Tragicomedy and mockery of justice,’ Forum 18 News Service, \url{www.forum18.org/archive.php?article_id=1894}.}

- On March 26, 2013, 22-year-old activist and member of the Azerbaijani Popular Front Party Dashgin Malikov was arrested on spurious drug charges following a number of Facebook posts in which Malikov openly criticized the government.\footnote{“Azerbaijan: Bogus Drug Charges to Silence Critics,” Human Rights Watch, May 27, 2013, \url{http://www.hrw.org/news/2013/05/27/azerbaijan-bogus-drug-charges-silence-critics}.} During a search at the police station, Malikov contends that drugs were planted in his wallet and that he was forced to sign a confession, which he later retracted. Malikov suffers from a medical condition that requires him to undergo bi-annual medical checks, none of which indicated any previous instances of drug use. In July 2013, Malikov was convicted and sentenced to two-and-a-half years in prison.

- Parviz Hashimli, a journalist from the local paper Bizim Yol and a director of the online platform Moderator.az, was detained on September 17, 2014. The following day, Hashimli received a two-month pre-trial detention sentence under articles 206.3.2 (smuggling of firearms on preliminary arrangement by an organized group) and 228.2.1 (illegally obtaining, storing, or carrying firearms and their spare parts on preliminary arrangement by an organized group) of the criminal code. On May 15, 2014, the journalist was sentenced to eight years in prison.

- Abdul Abilov, an online activist, was arrested on November 22, 2013 on charges of drug trafficking. On November 23, the activist received a three-month pre-trial detention sentence. Abilov is the founder of the Facebook page, “Let’s Say Stop to Flatterers.” The page was closed shortly after Abilov’s arrest. Abilov was also behind another Facebook page called “Election Fraud.” On May 27, 2014, the blogger was sentenced to five-and-a-half years in prison.

- Mikayil Talibov, an employee at a private bank, was convicted of libel in May 2013 for criticizing his former employer, AccessBank, on Facebook. Talibov had created a page on Facebook called “AccessBank-HaqszBank” (AccessBank-Unfair Bank),\footnote{“A resident of Astara is the first victim of defamation in internet,” Contact.az, August 14, 2013, \url{http://www.contact.az/docs/2013/Social/081400045887en.htm#.UtRP5vYmylx}.} which the bank considered to be libelous content. This case was the first time the new defamation law for online content had been applied. Talibov, a resident of the Astara region, was sentenced to one year of hard labor and retention of 20 percent of his salary. However, on January 24, 2014, the Astara District Court re-examined his case and made a decision to acquit the defendant.\footnote{“Astara resident acquitted by Astara District Court in the “Facebook” case,” Media Rights Institute, January 6, 2014, \url{http://www.mediarights.az/index.php?lngs=en&qid=86}.}

- 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 “Selections from AzTV,” with
some 57,000 followers. He is currently serving his three-month pre-trial detention. If convicted, he is facing up to three years in jail.

- On April 3, 2014, Baku Court of Grave Crimes found 20-year-old online activist Elsever Mursalli guilty under article 434.4.3 (illegal drug trade in large proportions) and sentenced Mursalli to five years in prison. Mursalli had criticized the Azerbaijani authorities on Facebook and was arrested on October 3, 2013. Another young man, Elvin Karimov, was detained shortly after and charged with illegal drug possession while his computer and phone were confiscated. He was running a Facebook page called “Azad Soz” (Free Speech) that posted political satire and had around 11,000 followers. If convicted, Karimov faces up to 12 years in prison.

In addition to detentions and prosecutions, the authorities have increasingly placed restrictions on individuals’ anonymity and privacy online. 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.

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 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.

Suspicions that the authorities monitor users’ online activity were confirmed by many of those detained for their involvement in the March 2011 protests, who reported that the authorities had referred to their Facebook activities and private communications during interrogations. This monitoring continues today, with arrested activists reporting seeing their Facebook message exchanges printed out. On February 27, 2014, Turkel Alisoy, a member of Popular Front Party’s youth

76 "Facebook activist sentenced to 5 years imprisonment," Contact.az, April 3, 2014, http://www.contact.az/docs/2014/Politics/04030007436Sen.htm#.U4e9HS_c0Xw
77
78
branch, was taken from his home to the Khatai District Police Office no. 35. From there, he was taken to the Baku City Main Police Office, where the head of the criminal investigation department showed him screenshots of his Facebook post in support of the Students' Day of Boycott Facebook event page. Alisoy reported that he was accused of intentionally calling students and other citizens to protest. During his temporary detention, Alisoy was threatened with criminal prosecution if he continued to call for protests on Facebook.80

In April 2012, a month before Azerbaijan was set to host the Eurovision Song Contest, a Swedish investigative documentary revealed evidence of a blanket mobile phone surveillance system employed by the telephone company Azercell.81 With help from the Stockholm-based telecom TeliaSonera, Azercell has reportedly installed “black box” devices on its networks that allow government security services and the police to monitor all mobile phone communications—including text messages, internet traffic, and phone calls—in real time without any judicial oversight. In addition, in an interview with a former employee of the technical team at the mobile company, it was revealed how Azercell has set aside special offices in their headquarters for government authorities to conduct surveillance activities.82 While it is unclear exactly when the monitoring system was installed and put into practice, one source working for TeliaSonera noted that “the Arab Spring prompted the regimes to tighten their surveillance...There’s no limit to how much wiretapping is done, none at all.”83

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 Team.84 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 Mamfakinch, by UAE authorities to spy on human rights activist Ahmed Mansoor, and more recently was used to target Ethiopian journalists in Washington, D.C.85

Netizens and their family members have also been subject to instances of extralegal intimidation and harassment through surprise police visits to their homes, summons to local branches of the Ministry of National Security for questioning, and arbitrary job losses.

Investigative journalist Khadija Ismayilova has been the victim of harassment multiple times. Known for her reporting on corruption in the country, including investigations into the president’s conduct and business activities, Ismayilova regularly disseminates her reports on social-networking sites such as Facebook, where she has a wide following. In May 2013, Ismayilova, along with other outspoken figures and opposition politicians, were the victims of a smear campaign when a pornographic website was launched just six months prior to the presidential elections and featured videos that

---

82 Interview took place in March 2014.
allegedly showed Ismayilova, opposition leader Ali Karimli, and others engaged in sexual acts (though in reality they are not the individuals in the videos). Called “Ictimayi Palatka” (Public Tent) the site is constantly updated, and no measures by the authorities have been taken to address the libelous content. In another incident on February 17, 2014, Ismayilova was questioned about a document she shared on her personal Facebook page, which exposed evidence of spies placed in political parties by the orders of the Ministry of National Security (MNS). The document originally was leaked to Ismayilova in 2011 by a former employee. On February 19, Ismayilova was informed of a criminal case opened against her under article 284.2 of the criminal code, “disclosure of state secret.” As of late 2014, she is not allowed to leave the country.

On October 2, 2013, just a few days before the presidential elections, photographer and video reporter Mehman Huseynov, who is also the founder of a popular satirical Facebook page “Sancaq,” was detained by the local police. Prior to his arrest, Huseynov posted a video mash-up of the voices of two presidential candidates from the televised pre-election campaign with a scene from the movie 300. The prosecutor general's office explained the detainment as part of an investigation into the “dissemination of information of a criminal nature on social networks,” specifying that the criminal information in this case was the “call” in the video that the “government must go.” Held and interrogated for over six hours, Hueynov was asked not to disseminate videos of such nature. On October 6, Huseynov’s own personal Facebook profile was blocked as a result of a series of violation reports sent from fake accounts. While Huseynov’s page was quickly restored, similar attempts took place on the day of the elections, when a popular Facebook page on elections was blocked.

Wrongful access to a computer, such as through the implantation of viruses or security breaches, is punishable under Chapter 30 of the criminal code. Internet security is also dealt with in the Law on National Security of 2004 and the Law on Protection of Unauthorized Information of 2004. Hacking attacks aimed at Azerbaijani internet users typically coincide with politically sensitive dates related to the unresolved territorial conflict between Azerbaijan and Armenia. Sometimes attacks occur after high-profile political statements. Some of these ostensibly Armenian-based attacks have targeted the websites of entities such as the MCIT, the National Library, and the public television broadcaster. The Anti-Cybercrime Organization is the main body working against cyberattacks in Azerbaijan, and the country ratified the Council of Europe’s Convention on Cybercrime in March 2010, which took effect in July 2010.

While certain opposition news websites such as Yeni Musavat, Radio Azadliq, and the personal blog of the Popular Front Party’s chairman Ali Kerimli have been subject to constant attacks that resulted in temporary shutdowns throughout the past few years, more recent attacks were also


87 YouTube Video, “Prezident seçkiləri 2013 - Cəmil Həsənli hamını məhv elədi” “Presidential Election 2013 – Destroying Hasanli,” accessed August 2014, [http://www.youtube.com/watch?v=-48PP8lxk9A](http://www.youtube.com/watch?v=-48PP8lxk9A). In the video, the voice of Jamil Hasanli, the candidate running against Aliyev, is saying through the voice of the main character “the government of Ilham Aliyev is up to its knees in corruption and Ilham Aliyev himself is up to his throat” ending with Hasanli saying “this government must go.”

88 Elections 2013 Facebook page, [https://www.facebook.com/secki.az](https://www.facebook.com/secki.az)


documented. On August 15, 2013, the web-editor of the Azadliq newspaper announced that the website Azadliq.info had been hacked. The DDoS attack was detected by the host server’s security service. In the past, opposition papers subject to attack have speculated that the cyberattacks were launched by the Ministry of Defense. The ministry, however, denies these allegations. The deputy editor of Olaylar.az, which has also suffered from cyberattacks, stated that the attacks increased in the months before the election. The Institute for Reporters’ Freedom and Safety (IRFS) also reported a cyberattack on their website on August 13, 2013. According to the institution, the website was targeted by a wide range of DDoS attacks, including Layer 7, UDP, SYN flooding, and DNS reflection attacks. Additionally, the sites of state bodies and state-controlled media have been subject to an increasing number of cyberattacks over the past year, with hackers targeting and defacing sites belonging to the Interior Ministry, the State Security Service, the Ministry of Education, and the ruling New Azerbaijan party, among others.

In December 2013, the Computer Emergency Response Team (CERT) in Azerbaijan announced that it would begin filtering the country’s incoming internet traffic in order to “protect the entire perimeter” of the internet in Azerbaijan from cyberattacks and other malicious threats. CERT is a body that functions under the State Agency for Special Communication and Information Security of Special State Protection Service.

---

Bahrain

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>35</td>
<td>35</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>72</td>
<td>74</td>
</tr>
</tbody>
</table>

Population: 1.1 million
Internet Penetration 2013: 90 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

* 0=most free, 100=least free

Key Developments: May 2013 – May 2014

- ISPs restricted access to Whatsapp, Viber, and Skype in advance of the August 14, 2013 'Tamarod' demonstrations, disrupting online mobilization. Internet speeds were also throttled ahead of the three-year anniversary of country-wide protests on February 14, 2014 (see Obstacles to Access).

- A government initiative to censor “terrorist materials” resulted in the blocking of at least 70 websites, including many that feature content from political opposition or Shiite religious groups. Orders were also issued to monitor and filter text messages coming from abroad (see Limits on Content).

- At least 23 online users were arrested for offenses such as calling for protests or insulting the king on social media. Twelve have been found guilty thus far, with courts sentencing users to longer jail sentences in comparison to last year. A 10-year sentence was given to Abdali Khair for forwarding a Whatsapp message containing a statement of the opposition February 14th Coalition, now branded a terrorist group (see Violations of User Rights).

- A Cyber Safety Directorate was established, consisting of employees from government ministries and telecom companies, to monitor websites and social media for content that instigates violence or terrorism or disseminates lies and fallacies that pose a threat to the kingdom. Authorities sent links to opposition social media accounts which traced the user’s IP address when clicked (see Violations of User Rights).
Introduction

Over the past year, renewed calls for protest and a tamarod (“rebellion”) led to the throttling of internet speeds around key events, the temporary blocking of social media and communication apps, and the blocking of websites linked to the political opposition and Shiite groups. New regulations that would restrict online freedom are underway, including a cybercrimes law that would criminalize establishing a website to promote “the disruption of public order”. A combined total of 360 months (30 years) of prison sentences have been passed down on twelve Bahraini citizens as a result of their ICT activities, of which the longest was ten years. Users were handed one-year jail terms; similar cases the year before resulted in six-month sentences.

Surveillance of online activity and phone calls, combined with the continued crackdown on users, is pushing more Bahrainis toward self-censorship. Numerous users arrested for social media posts, particularly on Twitter, reported being subject to physical or psychological torture while held by authorities. Blogger Mahamed Hasan fled the country and applied for political asylum after his arrest and torture. Finally, online activists are subject to consistent cyberattacks, including targeting with spy links to expose their identity using fake accounts operated by the government.

In the absence of a representative government, many Bahrainis look to the internet as an outlet for expressing political, economic, and social frustrations in the country. 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. In 1997, only two years after the internet was introduced in the country, a Bahraini internet user was arrested for the first time after sending information to a political opposition group outside of the country.1

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.2 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.3 The Ministry of Information made its first official attempt to block websites containing content critical of the government in 2002, and as of 2009 at least 1,000 websites were blocked, including individual pages on certain social-networking sites.4

Obstacles to Access

From a technological perspective, Bahrain is one of the most highly connected countries in the world. In 2013, Bahrain ranked third in the Arab region on the 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 many applications available in Arabic, and a high level of English language knowledge. The number of internet users has risen rapidly, from a penetration rate of 33 percent in 2007 to 90 percent in 2013. As of the first quarter of 2014, there are approximately 1.7 million broadband subscriptions in the country, of which 90 percent were mobile broadband. Dial-up connections disappeared in 2010 and ADSL use has declined with the growth of mobile broadband. Broadband prices fell by nearly 53 percent between 2011 and 2012, and are among the lowest in the region for low usage mobile broadband. However, prices are high for residential broadband in comparison to countries in the Organization for Economic Cooperation and Development (OECD).

Bahrain also has one of the highest mobile phone penetration rates in the region at 166 percent as of the end of 2013, representing over 2.2 million subscribers. BlackBerry phones are popular among young people and the business community and account for around 13 percent of mobile subscribers, even though authorities banned BlackBerry users from sending news bulletins through text messages in 2010. 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.

On August 14, 2013, the day when Bahrain’s Tamarod (“rebellion”) protests were planned to take place, the authorities banned BlackBerry users from sending news bulletins through text messages.

---

place, reports indicated that Whatsapp, Viber and Skype were temporarily blocked on multiple internet service providers (ISPs) for several hours. Users also reported abnormally slow internet speeds.\textsuperscript{15} Authorities also throttled internet speeds on February 13, 2014,\textsuperscript{16} in conjunction the anniversary of the February 14 protests, as well as a Twitter campaign calling on U.S. President Barack Obama and the UN Secretary-General Ban Ki-moon for support.\textsuperscript{17}

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."\textsuperscript{18} The TRA fined a main operator VIVA in August 2013 for exceeding the bandwidth limitations set out in its frequency license.\textsuperscript{19} The TRA has also issued several regulations that have not been welcomed by consumers, including measures that violate individual privacy.\textsuperscript{20} (See “Violations of User Rights”)

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).\textsuperscript{21} 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. Two marginal ISPs stopped providing internet services in 2013; the reason is unclear.\textsuperscript{22} In March 2013, the TRA limited a tender for additional frequency bands to support the launch of 4G LTE to major ISPs Batelco, Zain and VIVA that also act as the only mobile operators in Bahrain.\textsuperscript{23} In April, a court accepted an appeal

\textsuperscript{15} “On #Bahrain Tamarrod day: Internet slow, Chatting apps blocked”, Bahrain Index, August 2014 http://bahrainindex.tumblr.com/post/58264073435/on-bahrain-tamarrod-day-internet-slow-chatting-apps

\textsuperscript{16} “Slow internet reported on the eve of the revolution anniversary”, Bahrain Index, February 2014 http://bahrainindex.tumblr.com/post/77604642724/slow-internet-reported-on-the-eve-of-the-revolution

\textsuperscript{17} “Campaign in Bahrain calls on Obama to intervene in favor of the opposition” [in Arabic], Radio Sawa, February 14, 2014 http://www.radiosawa.com/content/%D8%A9%D9%85%D9%84%D8%A9-%D8%AA%D8%B7%D8%A7%D9%84%D8%A8-%D8%A3%D9%88%D8%A8%D8%A7%D9%85%D8%A7-%D8%8D%D8%A7%D9%84%D8%AA%D8%AF%D8%AE%D9%84-%D9%84%D8%A7%D9%84%D9%85%D8%B1%D8%A7%D8%B6%D8%A9-%D8%A7%D9%84%D8%A8%D8%AD%D8%B1%D9%8A%D9%86%D9%8A%D8%A9/-243612.html


\textsuperscript{21} In June 2013, Mohamed al-Rumaihi was named President of the IAA, replacing Fawaz al-Khalifa who remained Minister of State for Telecom.


\textsuperscript{23} “Bahrain’s 4G auction further delayed by dispute “, CommsMEA, April 7, 2013 http://www.commsmea.com/13166-bahrain-4g-auction-further-delayed-by-dispute/
from Menatelecom, a major ISP, to be included in the tender, forcing the TRA to cancel it in June. Subsequently, in September, the TRA started providing LTE frequencies to all requestor operators. Two ISPs, VIVA and Menatelecom are also licensed to provide the increasingly popular WiMax technology for accessing wireless broadband from one’s computer through a USB device.

The government has a controlling stake in Bahrain’s largest telecommunications company, Batelco, while other ISPs are owned by investors from the private sector, including non-Bahraini investors. Although there is no centralized internet backbone in Bahrain, all ISPs are indirectly controlled by the government through orders from the TRA. This tight control over the country’s ICT sector has allowed the Bahraini authorities to enforce strict limits on online content.

**Limits on Content**

Over the past year, the scale of censorship increased, while the level of sophistication remained stable. At least 70 websites were blocked and new orders were given to service providers to filter text messages. Increased self-censorship caused a notable drop in the number of Bahraini social media users.

Multiple state organizations, including the IAA, Ministry of Interior and Ministry of State for Telecommunication can order the blocking of a website without referring the case to a court. The IAA blocks websites that violate Articles 19 and 20 of the country’s Press Rules and Regulations. This includes 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.” Any site that criticizes the government, the ruling family, and the country’s status quo is subject to blocking by the IAA. According to an online community-based survey, 39 percent of all sites reported blocked in 2014 were related to politics, while 23 percent were related to the use of various internet tools, such as anonymizers and web proxies.

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

---

24 “«Mena Telecom» wins a court order to stop an auction procedures of the fourth generation until the company is allowed to enter”, alwasat news, April 17, 2013 http://www.alwasatnews.com/3875/news/read/764831/1.html.
Coat technology. In 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. It is unclear whether or not the tools have been implemented, but in December 2013 the company signed a deal with a distributor that covers Bahrain’s market.

According to estimates dating from 2009, the IAA had blocked or shut down at least 1,000 websites, including human rights websites, blogs, online forums, and individual pages from social media networks. Many more websites were blocked after the 2011 protests, which was called for and heavily covered by online channels, resulting in a significant rise of blocking and filtering measures by the Bahraini authorities. 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.

Although there are a number of news websites providing a plurality of viewpoints distinct from the narrative of Bahraini state media, 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.

In August 2013, the communications minister ordered ISPs to block 70 websites, 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. A hotline and an email account were established to receive reports.
on abusive and terrorist social media pages.\textsuperscript{40} 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.\textsuperscript{41} Although the full list of blocked websites was not made available, news sites affiliated with Bahrain’s popular February 14th Coalition protest movement, and online forums linked to the political opposition and the main religious group “Olama Islamic Council,” were also affected.\textsuperscript{42}

YouTube, Facebook, Twitter, and international blog-hosting services are freely available. However, certain 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.\textsuperscript{43} PalTalk, a chatting service that was used to conduct political seminars for wide online audiences, has been blocked since June 2011.\textsuperscript{44} This intensified 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.\textsuperscript{45} Following the circulation of photos online showing Bahraini schoolyards filled with water after heavy rainfall, the Ministry of Education banned all school directors from publishing any photos online without permission.\textsuperscript{46} Separately, a website that broadcasts public events of political opposition groups was blocked on November 23, 2013, during a conference on the implementation of recommendations from the Bahrain Independent Commission of Inquiry.\textsuperscript{47}

Authorities also use extralegal measures to forcibly remove online content. Through the use of arrests,\textsuperscript{48} detentions, and torture,\textsuperscript{49} security forces coerced many online forum moderators into

\begin{itemize}
\item \textsuperscript{40} “Ministry of State for Communications To Regulate Websites Linked to Internationally Recognized Terrorist Organizations”, Bahrain News Agency, August 3, 2013 http://www.bna.bh/portal/en/news/573944
\item \textsuperscript{41} The websites of Al-Qaeda and Al Nusrah Front remain accessible as of 10 Jan 2014, \url{http://bahrainindex.tumblr.com/post/57447600168/ministry-of-state-for-communications-to-block-70}
\item \textsuperscript{42} In September 2013, one month after the blocking order, a court ruled that the February 14th Coalition is a terrorist group. The Olama Islamic Council was dissolved by a court in January 2014 for allegedly inciting violence.
\item \textsuperscript{43} These sites include livestream.com, bambuser.com, ustream.tv, justin.tv, and other websites that stream directly to Twitter like twitcasting.tv and twitcam.livestream.com. See, “Attacks on media continue across Middle East,” Committee to Protect Journalists, February 16, 2011, \url{http://en.rsf.org/bahrain-crackdown-continues-in-bahrain-16-06-2011,40467.html}.
\item \textsuperscript{44} “Bahrain: The “Cyber Safety Directorate” Monitors Internet Activity In Style Similar to Big Brother “, Bahrain Center for Human Rights, November 25, 2013 \url{http://www.bahrainrights.org/en/node/6624}
\item \textsuperscript{45} “Bahrain: Schools ‘need ministry approval’ to publish news”, BBC, November 25, 2013 \url{http://www.bbc.co.uk/news/blogs-news-from-elsewhere-25088333}
\item \textsuperscript{46} “Bahrain: The “Cyber Safety Directorate” Monitors Internet Activity In Style Similar to Big Brother “, Bahrain Center for Human Rights, November 25, 2013 \url{http://www.bahrainrights.org/en/node/6624}
\item \textsuperscript{47} “Bahrain: Twitter User Jailed for 66 Days for Tweeting “, Global voices, December 5, 2011 \url{http://globalvoicesonline.org/2011/12/05/bahrain-twitter-user-jailed-for-66-days-for-tweeting/}
\end{itemize}
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 made available only through 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 May 2013, progovernment users led a mass campaign to compel Instagram to close the page run by al-Wefaq by submitting complaints to the photo-sharing app and website. Al-Wefaq is the largest political group in Bahrain and uses its account page to publish photos of attacks on protestors by security forces. According to Google, Bahrain requested the removal of one YouTube video for “security and privacy” reasons in the period between January and June 2013, but the company did not comply. Twitter’s Transparency Report reveals no requests from Bahraini authorities.

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.

Authorities also manipulate online content in order to fabricate greater public support. The independent group Bahrain Watch lists 18 PR firms known to have been hired by the government for promotional campaigns since February 2011, representing at least $32 million in contracts. Hoax journalists spread propaganda on Twitter and progovernment blogs such as Bahrain Views and Bahrain Independent. At least one PR agency was contracted to provide “web optimization and blogging” services, while others were hired for online reputation management. Multiple Wikipedia entries linked to Bahrain were changed in favor of the government. Similarly, an “army

---

50 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 AlAsheeri forever” [in Arabic], Bahrain Mirror, January 4, 2012, http://bhmirror.no-ip.org/article.php?id=26788&cid=117.
53 See https://transparency.twitter.com/.
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 moderately effective in silencing or reducing the activity of opposition voices 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 (See “Violations of User Rights.”) In September 2013, a fake WikiLeaks cable was published on a Bahraini progovernment forum with the objective of defaming a Bahraini member of parliament (MP) who had spoken out against the crackdown on protests. The Chamber of Deputies (Majlis an-nuwab) was prepared to take action against the MP for violating his parliamentary duties, until it was revealed that the cable was fake. 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.”

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

---

68 “Bahrain Govt using fake Twitter accounts to track online critics”, Bahrain Watch, July 31, 2013 https://bahrainwatch.org/blog/2013/07/31/bahrain-govt-using-fake-twitter-accounts-to-track-online-critics/.
Bahrain

is difficult for blocked websites to secure advertising, popular sites such as Bahrain Online 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 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. 72 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. 73 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. 74 The number of Bahraini users on Facebook dropped 16 percent to 345,520 as of May 2013, 75 representing a penetration rate of 25 percent. 76 The number of active Bahraini Twitter users also continued to drop, 77 from 72,468 reported in June 2012, 78 to 64,300 in March 2013, 79 and 62,200 in March 2014. 80 Following the prosecution of four internet users in 2012, 81 use of the #Bahrain hashtag also dropped. 82 Despite this, the hashtag remains one of 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 (نايرحبلا) in March 2014 alone. 83

Indeed, the internet is also the main source of information and news for many Bahrainis, particularly those active on Twitter. Given restrictions on press freedom, the lack of international media coverage,
and the inability of many prominent journalists to enter the country, activists use digital tools to bring attention to protests and human rights violations. The resilient social protest movement titled the “Coalition of February 14 Youth” continues to use social networks, both to organize protests and bring international mainstream media attention to local causes. For example, on February 17, 2014 the BBC reported 13,000 followers for an Arabic hashtag "bloody_Thursday," referring to the violent attack on protestors at Bahrain’s Pearl Roundabout on February 17, 2011. YouTube videos are also uploaded to document police attacks on civilians and torture testimonies, though some are promptly blocked. Relatives or friends of detainees regularly use Twitter to campaign for their release and provide updates about prison conditions. Overall, by uploading videos and sharing images on social media, protesters have maintained the spotlight on their struggle.

**Violations of User Rights**

The past year has witnessed an increase in violations of user rights. Authorities stepped up arrests of Twitter users for expressing criticism of the government or calling for protests online. Also increasing is the practice of targeting activists with surveillance malware in order to monitor their online activities and collect personal information. The legal environment remains an impediment to freedom online, although authorities also make use of extralegal measures such as arbitrary detention and torture to intimidate and prosecute users. Bahraini authorities have continuously called for more restrictions on internet freedom in recent years.

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." 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 law.” 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. 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.

Numerous regulations related to the internet proposed since 2011 signal a negative trend in the country's legal environment. Official announcements in 2012 signaled preparations to introduce tough new laws to combat the “misuse” of social media, after information spread online about the identities of security officers involved in human rights violations. In July 2013, a special national assembly of the House of Representatives recommended toughening penalties for social media users who “disseminate false information to foreign actors.” Fulfilling a commitment for a unified GCC system to combat cyber-crimes, 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. The Ministry of Interior is currently drafting the law. A proposed computer crimes law has been under review since 2005 and is currently going through final review by a Shura Council committee, before releasing it for votes at lower house of parliament.

Online censorship and criminal penalties for online speech are currently enforced under the 2002 Press and Publications Law, which does not specifically mention online activities but was extended to mobile telephones in 2010. The law allows for prison sentences of six months up 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. In addition, the 2002 Telecommunications Law contains penalties for several online practices such as the transmission of

---

99 A unified system to combat cyber-terrorism and enhance cyber-security in the GCC was approved by the GCC Supreme Council in its 33rd session in Bahrain in December 2012.
messages that are offensive to public policy or morals. 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 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.

After the March 2011 crackdown, the government conducted a mass arrest campaign of online activists and bloggers. Arrests and prosecutions continued throughout 2012 and 2013. Between May 2013 and April 2014, at least 23 online users were arrested, detained and prosecuted for their ICT activities. Collectively, 360 months (30 years) of prison sentences were passed down to twelve Bahraini users in cases directly related to online posts between May 2013 and April 2014. As photos and videos of police brutality continue to emerge online, more measures are being taken against citizens who are seen holding cameras, including smartphones, in protest areas. Bloggers, moderators, and online activists are systematically detained and prosecuted by authorities for expressing views the government regards as controversial.

Many prosecutions during the coverage period involved Twitter. In March 2013, six Twitter users were arrested, in nighttime raids, for using terms such as “dictator” or “fallen one” when referring to the king in anonymous posts. None of the users had a large base of followers. Instead, it seemed that the authorities selected them in order to instill fear locally, without provoking criticism from the international community. In May, five were sentenced to one year imprisonment under article 214 of the penal code, which relates to defaming the king and symbols of the kingdom. One, Ammar Makki, said he was threatened with torture in order to force a confession. On June 25, 2013, the sixth user, 17-year-old Ali al-Shofa, received the same sentence on the same charge. Al-Shofa said he had only retweeted others’ messages. He appealed the verdict, but was arrested on October 4, 2013; his sentence was upheld in December. Sentences passed in 2012 for the same

109 “Prosecution: the imprisonment of 5 for a year for misuse of the right to freedom of expression against His Majesty the King through “Twitter” and acquittal of the sixth” [in Arabic], Alwasat News, May 15, 2013 http://www.alwasatnews.com/3903/news/read/772574/1.html
111 Bahrain Penal Code, Article 214 “A prison sentence shall be the penalty for any person who offends the emir of the country [the King], the national flag or emblem” http://www.bahrainrights.org/sites/default/files/Bahrain-Penal-Code.doc

109 www.freedomhouse.org
charge did not exceed six months.115 Worryingly, in April 2013, the parliament introduced legislation to increase penalties related to insulting the king to a maximum of five years.116

The six users ran their social media accounts anonymously. Their identities were discovered using malicious spy links which tracked the users’ IP address when clicked and were sent from Twitter and Facebook accounts that impersonated well-known opposition figures or other friendly individuals.117 However, IP tracking is unreliable, as it targets the owner of an internet connection, rather than the operator of a specific social media account. In 2014, after the anonymous operator of the @karranah14 Twitter account clicked a malicious link, authorities raided the home of Mahdi al-Basri. The operator told Bahrain Watch he had used al-Basri’s connection. Al-Basri was not associated with the account, but served a one year prison sentence nonetheless.118

At end of July 2013, two weeks before the planned tamarod protests, the security forces carried out a campaign of arrests to intimidate online and offline activists. Blogger Mohamed Hasan (@safybh) had his house raided at 3am on July 31, 2013 by masked security agents. With no warrant, he was arrested, had his electronic devices confiscated, and was held incommunicado for over three days.119 During that period he was subjected to torture at the criminal investigation department in a bid to force his confession. He was reportedly “beaten with fists and a plastic hose, kicked, threatened with electric shocks, forced to strip naked and had his clothes taken away.” The agents threatened to rape his sisters and prevented him from sitting down, sleeping or eating.120 His lawyer, Abdul Aziz Moussa, was unable to see him until August 7, 2013, during interrogation by the public prosecutor. Moussa was detained that same day, shortly after he had tweeted of seeing signs of torture on Hasan’s arms.121 He was released on bail and, as of May 2014, was awaiting trial on charge of publishing a “defendant’s names without permission and the disclosing of investigation secrets.”122

Mohamed Hasan was released on bail on October 3, 2013. His charges include “calling for illegal gatherings, inciting hatred against the regime, inciting people to ignore the law, and misuse of social media.”123 This was the second time Mohamed was interrogated for his online activity; in 2012 he was interrogated for “writing for websites and newspapers without a license, protesting, and

tweeting,” although there is no law in Bahrain that requires a license for blogging. He suspended his blogging activity in April 2013. In February 2014, it was revealed that he has left Bahrain and sought political asylum in the UK.

On May 27, 2014, the public prosecutor announced an investigation into two individuals suspected of involvement with the Twitter account @mnarfezhom, a 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.” The prosecutor said that the two users were arrested from an office preparing videos to post online. The main operator of the account is a royal family member, Mohamed Salman Saqer al-Khalifa. The account began by reporting on protestors and defaming opposition figures, but eventually evolved, attacking other progovernment groups of differing opinions. It consistently published important news before any official source, including the move to revoke 31 Bahrainis’ citizenship and the death of an Emirati citizen working with the Bahraini riot police. Although many have lodged complaints with the public prosecution against the account, no action had been taking during the past three years. Things appear to have changed when @mnarfezhom posted that the Ministry of Interior 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 users were released the same day, and the account disappeared from Twitter one day later.

One of Bahrain’s most prominent human rights defenders, Nabeel Rajab, was released in May 2014 after completing a two-year sentence for “calling for illegal gatherings over social networks.” Rajab is the president of the Bahrain Center for Human Rights, a non-governmental organization that remains active despite a 2004 government order to close it. On December 2, 2013, the Court

124 See https://twitter.com/safybh/status/21005542406598657 (@safybh)
126 “Mohammed Al Khalifa, from an army officer to an arms dealer and eventually insulter of chaste women” [in Arabic], Alfateh news blog, October 26, 2012 https://alfatehnews.wordpress.com/2012/10/26/%D9%85%D8%A9%D9%85%D8%AF-%D8%A7%D9%84%D8%A9%D9%88%D8%A9-%D9%85%D9%86-%D8%B6%D8%A7%D8%A8%D8%B7-%D8%A7%D9%84%D9%89-%D8%AA%D8%A7%D8%AC%D8%B1-%D8%B3%D9%84%D8%A7%D8%AD-%D8%A7%D9%84%D9%89-%D8%B1/
127 “Twitter user of the ruling family in front of the judiciary in Bahrain” [in Arabic], Raseef22, June 2014 http://raseef22.com/News-Detail/1320/%D9%85%D8%A9%D8%B1%D9%91%D8%AF-%D9%85%D9%86-%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%8A-%D8%A7%D9%85-%D8%A7%D9%84%D8%82%D8%A7%D8%A7%D8%81-%D9%81%D9%8A-%D8%A7%D9%84%D8%AD%D8%B1%D9%8A%D9%86
130 Nabeel Rajab was first arrested on May 5, 2012 and held for over three weeks for “insulting a statutory body” in relation to a criticism directed at the Ministry of Interior over Twitter. On June 9, 2012, he was arrested again after tweeting about the unpopularity of the Prime Minister (also a member of the royal family) in the city of Al-Muharraq, following the sheikh’s visit there. A group of citizens from the city promptly sued Rajab for libel in a show of obedience to the royal family. On June 28, 2012, he was convicted of charges related to his first arrest and ordered to pay a fine of BHD 300 ($800). Shortly after he was released on bail, he was re-arrested on July 9, 2012 after a court sentenced him to three months imprisonment for the Al-Muharraq incident. The court of appeals later acquitted Rajab, although he had already served most of his sentence. However, he is currently serving a two-year sentence for “calling for illegal gatherings over social networks.”
of Appeals rejected a request for his early release without providing any grounds. His lawyers had argued that, in accordance with Bahraini law, he should be free to leave for good conduct after completing three quarters of his sentence.\textsuperscript{132} The Court of Cassation took over a year to set a date to look into his appeal, which it rejected in March 2014. Rajab, who tweets under the name ’@ NabeelRajab,’ was ranked the “most connected” Twitter user in Bahrain according to a survey, with over 150,000 followers at the time of his arrest in May 2012.\textsuperscript{133} He continued to issue calls to protest over Twitter, even from prison.\textsuperscript{134} By May 2014, Rajab’s followers had reached 231,000 and the tweet that originally led to his arrest had been retweeted at least 2,333 times.\textsuperscript{135}

Bahraini photographers who are active in documenting protests online have also faced reprisals. Award-winning photographer Ahmed Humaidan, who published photos over Flickr and Instagram, was jailed on December 29, 2012.\textsuperscript{136} He was placed in solitary confinement for a week and subjected to ill-treatment and psychological torture.\textsuperscript{137} In March 2014, he was sentenced to 10 years in prison for allegedly participating in an attack on a police station in the district of Sitra,\textsuperscript{138} though it is believed that his arrest is in fact due to him photographing protests.\textsuperscript{139}

Photographer Hussain Hubail and blogger Jassim al-Noaimi were arrested on July 31, 2013. Hubail was held incommunicado for over four days and was subject to torture at the criminal investigation department, where he was reportedly beaten with a plastic hose, kicked, deprived of sleep and food, and forced to listen while the blogger Mohamed Hasan, his friend, was tortured.\textsuperscript{140} Hubail suffers from a heart condition and has been denied adequate medical care in detention.\textsuperscript{141} On April 28, 2014, Hubail and al-Noaimi each received a five-year prison sentence on charges of “inciting hatred against the regime through social media, and calling for illegal protests” after a trial that lasted around five months.

On December 4, 2013, a Bahraini court held a hearing over the case of a defendant who was

\begin{itemize}
\item \textsuperscript{132} “The Observatory: Bahrain: The court’s decision not to grant Nabeel Rajab an early release is flawed”, The Observatory, December 4, 2013, \url{http://www.bahrainrights.org/en/node/6635}.
\item \textsuperscript{133} “How the Middle East Tweets: Bahrain’s Most Connected,” Wamda, December 3, 2012, \url{http://www.wamda.com/2012/12/how-the-middle-east-tweets-bahrain-s-most-connected-report}.
\item \textsuperscript{134} “Bitter protests in Bahrain,” Movements.org, January 28, 2013, \url{http://www.movements.org/blog/entry/bitter-protests-in-bahrain/}.
\item \textsuperscript{135} “Khalifa: Leave the al-Muharraq alley ways, their shaikhs and their elderly, everyone knows that you have no popularity there; and if it was not for their need for money they would not have come out to welcome you - When will you bow out?” \url{https://twitter.com/nabeelrajab/status/208853736494350336}.
\item \textsuperscript{136} See: \url{http://instagram.com/ahmedhumaidan/}, \url{http://www.flickr.com/photos/86494560@N05/}, and \url{http://500px.com/AhmedHumaidan}.
\item \textsuperscript{137} See \url{https://twitter.com/BHRS2001/status/287932501744304128}; “Fake bomb in the hands of photographer Humaidan in order to extract confessions” [in Arabic], Bahrain Mirror, January 12, 2013, \url{http://www.bahrainmirror.com/article.php?id=7365&cid=73}.
\item \textsuperscript{138} “Public Prosecution / Statement,” Bahrain News Agency, January 5, 2013, \url{http://www.bna.bh/portal/en/news/54055}.\textsuperscript{138}
\item \textsuperscript{139} “Bahrain arrests photographer who documented dissent,” Committee to Project Journalists, January 9, 2013, \url{http://www.cpi.org/2013/01/bahrain-arrest-photographer-who-documented-dissent.php}.
\item \textsuperscript{140} “NGOs Submit Letter of Allegation Concerning The Detention Of Journalist Mohammed Hassan, Photographer Hussain Hubail And Cameraman Qassim Zain Aldeen”, Bahrain Center for Human Rights, December 16, 2013 \url{http://bahrainrights.org/en/node/6657}.
\item \textsuperscript{141} “Bahrain: Detained Photographer Hussein Hubail Brought To Court Amid Deliberate Neglect To His Health Condition”, Bahrain Center for Human Rights, December 7, 2013 \url{http://bahrainrights.org/en/node/6638}.
\end{itemize}
arrested for holding illegal gatherings and “insulting the king using photos over Instagram.” The public prosecution claimed that the defendant “confessed” the latter crime during interrogation.¹⁴²

Photographer Ahmed Al-Fardan, who uses photo-sharing platforms like Instagram and Demotix, was briefly arrested at a cafe on August 8, 2013, by plainclothes police. He was subsequently beaten and threatened with death unless he cooperated in providing photos of demonstrators.¹⁴³ In the early hours of December 26, 2013 he was again arrested without a warrant and disappeared for over a week. He was subject to torture that resulted in two broken ribs,¹⁴⁴ and interrogated without a lawyer present on charge of “intending to participate in illegal gatherings.”¹⁴⁵ On January 9, 2014 he was released, following pressure from international media watchdogs.¹⁴⁶ His trial began in May 2014.

Other users were prosecuted for text messages over mobile chatting applications like Whatsapp. On March 2014, a man was sentenced to one year in prison for insulting the prophet’s companion over a Whatsapp message, a form of sectarian hate speech against Sunni Muslims’ who honor these religious figures. He was reported to the police by the receiver of the message.¹⁴⁷ Online hate speech against religious figures dignified by Shia Muslims often takes place with impunity:¹⁴⁸ On a different case, the political opposition society al-Wefaq was ordered to pay a compensation of BHD 1,500 (US$ 3,980) in March 2014 to a lawyer who claimed that he was “psychologically hurt” after receiving a text message from al-Wefaq calling him to join the protests at the pearl roundabout in February 2011.¹⁴⁹

One of the harshest sentence during the reporting period was passed on September 29, 2013, when a Bahraini court sentenced Abdali Khair to 10 years in prison under the terrorism law for forwarding a message on Whatsapp that contained a statement from the opposition youth movement, the February 14th Coalition.¹⁵⁰ He was put on trial along with a group of 50 people on charges related to their involvement in the Coalition, including terrorism, without having interrogated or even notified

---

¹⁴⁷ “Man sentenced to prison for insulting prophet’s companion over whatsapp”, March 5, 2014 http://bahrainindex.tumblr.com/post/78659749504/man-sentenced-to-prison-for-insulting-prophets
¹⁴⁸ See: a snapshot of a tweet by pro-government account (@Mnarfezhom) referring to Imam Hussain grandson of Prophet Mohamed as “pig” [in Arabic] https://twitter.com/BuHSN/status/158147589609504768
¹⁴⁹ “Court ordered ‘Alwefaq’ to pay compensation to a lawyer who have received a phone message calling for participation in «the roundabout»”, AlWasat News, March 31, 2014 http://www.alwasatnews.com/4223/news/read/871407/1.html
¹⁵⁰ “Abdali Khair” receives 10 years prison sentence for forwarding a statement on the Whatsapp” [in Arabic], AlWefaq, October 2, 2013, http://alwefaq.net/cms/2013/10/02/23233/
Khair of the charges. According to local and international human rights observers, the trial fell far short of international standards.

Bloggers also faced prosecution. In April 2014, blogger Ali Miaraj was sentenced to two years' imprisonment for insulting the king and an additional six months for misusing telecommunication tools. He was detained in January 2014 for writing and posting articles on the antigovernment website luluawal.no-ip.org, which has been blocked since its launch in 2012. The trial took only three hearings and no defense witnesses were allowed to testify.

The two harshest sentences ever passed on Bahraini bloggers remain in place, after the Higher Court of Cassation upheld a 2011 ruling by a military court in January 2013. Two bloggers, Abduljalil al-Singace and Ali Abdulemam, were charged with possessing links to a terrorist organization aiming to overthrow the government, 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, and his blog has been blocked since 2009. Abdulemam, the owner of Bahrain's popular blocked online forum, Bahrain Online, received a 15-year sentence in absentia and is currently a political refugee in the UK. He had previously spent two years in hiding in Bahrain. Both have been subject to torture.

In other cases, the government has used extra-legal methods to punish users for their online posts. On August 10, 2013, Bahrain deported Erin Kilbride, a U.S. citizen working as a teacher, because of her online activity. Two days earlier, an article written by Kilbride under a penname had been published on Voice of America. The Bahraini authorities claimed that Kilbride's multiple posts “incite[d] hatred against the government and members of the Royal family” and that she was spreading misinformation and encouraging divisions in Bahraini society based on religious sect.

The Bahraini authorities are remarkably responsive when enforcing the country's tight online restrictions. At around 3am on June 20, 2013, Twitter user Jafar Al-Demstani (@alidemstani) was subject to arbitrary arrest during a house raid performed by armed and masked security forces in

---

151 Abdali Khair went to the hearing on July 25, 2013 only after seeing his name published in a wanted list by the Ministry of Interior. He was quickly arrested.


plain clothes. Twelve hours earlier, he had tweeted that his imprisoned father suffers from a back injury due to the torture he received at the hands of Colonel Mubarak ben Huwail, an officer known for being protected by the prime minister. Al-Demstani was kept in detention until July 15, 2013, initially without anyone’s knowledge, and was released without charge.

Since 2011, students and employees have received disciplinary action for comments they have communicated via private text messages and social media. On November 23, 2013, a court fined a user BHD 100 (US$ 265) for “insulting his work manager” over Twitter. He had posted anonymous tweets accusing his manager of corruption and calling him a thief. The manager filed a complaint with the police who traced his IP address.

Given that the authorities have been quick to identify social media users who operate under a pseudonym, many users are concerned about restrictions on using 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 must 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 access to subscriber data upon request. After the application of the National Safety Status emergency law in March 2011, security personnel began searching mobile phones at checkpoints, behavior that was documented on YouTube. On December 19, 2013, Mohamed Mushaima was interrogated over “banned pictures and videos of the revolution” that were found on his mobile phone. He was released but was informed his case would be taken to the public prosecutor. According to Facebook’s Transparency Report, the Bahraini
In November 2013, a new Cyber Safety Directorate at the Ministry of State for Telecommunications Affairs was launched to monitor websites and social media networks, in order 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 monitoring of Instagram resulted in the arrest of four users accused of running an account that defamed religion in February 2014. They were charged with misusing telecommunication and defaming Prophet Mohammed’s comrades through “the use of abusive images of the caliphs of Islam and by posting immoral photos.” The IAA also 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 Bahraini cyberspace is highly monitored, less action is taken against the dozens of progovernment users who make threats online against activists, and even the U.S. ambassador to Bahrain. Some identify protestors and circulate lists of “traitors” on social media. No action has taken against them by the public prosecution, though their targets have accused them of defamation. It is common for users tied to the opposition movement to receive this type of harassment in a bid to disrupt their activities. Activist Said Yousif al-Muhafda chose exile after receiving death threats over Twitter.

In July 2012, researchers discovered malicious software concealed in seemingly innocent emails sent to Bahraini activists in April and May. The surveillance software, FinFisher, is developed by the Munich-based Gamma International and distributed by its U.K. affiliate, Gamma Group. One aspect of the software, FinSpy, can remotely take control of a computer, taking screen shots, intercepting VoIP calls, and transmitting 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

176  “Former Bahraini colonel threatens the U.S. ambassador to apply «religious duty» on him” [In Arabic], Bahrain Mirror, October3, 2013 http://bahrainmirror.com/news/11449.html?utm_medium=twitter&utm_medium=twitter
Bahrain

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.\(^{181}\) 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.\(^{182}\) In July 2013, links to a website apparently soliciting signatures in support of the rebellion were distributed over social media. In reality, the website was collecting identification user data, including IP addresses.\(^{183}\)

Cyberattacks against both opposition and progovernment pages, as well as other websites, are common in Bahrain. For example, in July 2013, multiple Twitter accounts affiliated with the opposition were hacked.\(^{184}\) According to official statistics, there were 208 daily cyberattacks during January 2014 on government websites in attempt to take over the sites or manipulate content. Additionally, at least 40 sources of malicious email were identified inside Bahrain by MacAfee.\(^{185}\) Government-associated websites are frequently targeted with distributed denial of service (DDoS) attacks, with the most recent instance occurring on August 14, 2013 the day of planned rebellion protest in Bahrain.\(^{186}\) The main perpetrator of such attacks has been the group “Anonymous,” which launched “Operation Bahrain” through a press release published on February 17, 2011.\(^{187}\)

181 “You Only Click Twice: FinFisher’s Global Proliferation,” CitizenLab, May 13, 2013, [https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/](https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/).


Bangladesh

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>Partly Free</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Partly Free</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td>Partly Free</td>
<td>49</td>
<td>49</td>
</tr>
</tbody>
</table>

* 0 = most free, 100 = least free

Population: 156.6 million

Internet Penetration 2013: 6.5 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- The government amended the controversial ICT Act to allow warrantless arrests and maximum 14-year jail sentences for violations on social, political, and religious issues online (see Violations of User Rights).

- In June 2013, a court condemned an absconding university lecturer to two years in prison under the penal code for threatening the prime minister—and an additional five years under the ICT Act for doing so on Facebook (see Violations of User Rights).

- In September, a court formally indicted four bloggers for harming religious sentiment under the ICT Act (see Violations of User Rights).

- Police arrested an additional eight journalists, Facebook users, and civil society activists who criticized the government under the ICT Act (see Violations of User Rights).
Bangladesh

Introduction

Digital campaigning increased in Bangladesh prior to a national parliamentary election on January 5, 2014. 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. Its 2009 “Digital Bangladesh by 2021” program seeks to integrate internet access with development efforts in national priority areas, such as education, healthcare and agriculture. Private commercial stakeholders have also helped in the proliferation of net usage. Bangladesh further benefits from a vibrant—though 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. In June 2013, a court in the capital, Dhaka, sentenced a former university lecturer to two years in jail in absentia for threatening to kill the prime minister and an additional five years under the ICT Act for making the threat on Facebook; he is currently in hiding.

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. They were formally indicted in September for alleged anti-Islamic comments. By then, however, the penalties they faced had increased to a maximum 14 years in prison under an amendment passed in August 2013 without regard for civil society criticism. Police no longer need a warrant to make arrests under the amended act, and used it to detain at least eight bloggers, Facebook users, journalists, and civil society activists for criticizing the government or the prime minister during the coverage period of this report.

The crackdown came in the wake of demonstrations which some observers compared to the 2011 protests in Egypt’s Tahrir Square. These began in early 2013 when a domestic war crimes tribunal sentenced Abdul Quader Mollah, leader of the country’s largest political Islamic party Jamaat-e-Islami, to life imprisonment for crimes committed during the country’s 1971 war of independence with Pakistan. Tens of thousands of protesters gathered for several weeks around the Shahbagh intersection in Dhaka, where they were joined by different social, cultural and political forces. The Shahbagh Movement, as it became known, was facilitated by blogs and social networks, which Mollah’s supporters characterized as a conspiracy by “atheist bloggers.” After a pro-Jamaat-e-

References:
Bangladesh

Islami blog identified blogger Ahmed Rajib Haider as a Shahbag ringleader, armed assailants attacked and killed him outside his home in February 2013.

While no internet users were murdered in the past year, two teenagers were beaten by a mob in Chittagong for allegedly blasphemous comments on Facebook. Police intervened to rescue the teenagers, but arrested them under the ICT Act. Separately, multiple groups continued a disturbing practice of manipulating Facebook pages to suggest minority communities were insulting Islam, first used to incite violence against Buddhists in 2012. In November 2013, a Hindu in Pabna district was accused of maintaining an offensive Facebook page which was photocopied and distributed to incite a mob to destroy Hindu-owned residences, businesses and temples.

Censorship did not increase in the past year, but the arrests created a climate of intimidation that fostered self-censorship and mistrust. When controversial online data about personal wealth amassed by politicians up for re-election became inaccessible, many accused the Bangladesh Election Commission of purposely throttling their own webpage at the government's behest. The Commission attributed the disruption to technical error.

Obstacles to Access

The International Telecommunication Union reported internet penetration in Bangladesh at 6.5 percent in 2013. Government estimates were closer to 20 percent.

Approximately 96 percent of users access the internet via mobile phone, 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 3 percent), or via one of the three wireless WiMax operators (1 percent). In 2014, 61 ISPs were operating nationwide as members of the official industry body, the ISP Association of Bangladesh.

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. By 2011, the government established 4,501 centers around Bangladesh providing cost-effective internet access and related e-services in poorer communities.

---

Bangladesh

Mobile penetration was at 67 percent in 2013, with connections provided by six operators. Grameen Phone, owned by Telenor, is the market leader with 42 percent of the total customer base, followed by Orascom’s Banglalink with 25 percent, and Robi, under the Axiata company, with 23 percent. The remaining three, Airtel, Citycell, and the state-owned Teletalk have a total customer base of 10 percent. As of 2014, all except Citycell offered 3G services.

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. In addition, the ability to access localized information and create content in Bengali has contributed to the popularity of local blog hosting services.

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. 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 from the information superhighway.

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. This move created administrative delays in a number of basic processes like the announcement of new tariffs or license renewals. Recently, the Ministry of ICT merged with the Ministry of Post and Telecommunications, with the goal of streamlining many ongoing projects and related industries. 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.

---

17 Interview with Syeda Gulshan Ferdous Jana, founder of Somewhereinblog, 2013.
18 Hussain, “ICT Sector Performance Review for Bangladesh.”
Limits on Content

The BTRC unblocked YouTube at the start of the coverage period after blocking it in 2012 in relation to the Innocence of Muslims video clip. Campaigners across the political spectrum embraced digital tools in advance of the January election, but news reports accused the Bangladesh Election Commission of slowing or throttling access to online data about assets belonging to Awami League politicians. There were no reports of state manipulation of online content, but a Facebook page containing a religious insult led to violent attacks on a Hindu community in Pabna district at the end of 2013. A 2013 amendment to the ICT Act discussed in Violations of User Rights also increased self-censorship online.

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, internet news providers do not have the government recognition granted to traditional, licensed press organizations, leaving them in a regulatory limbo. International companies are also subject to requests. In the second half of 2013, Facebook restricted access to three different pieces of content, "reported under local laws prohibiting criticism of the state."

International social media and communication apps are regular victims of government censorship in Bangladesh. Facebook was blocked for periods ranging from a few hours to a few days at a time in 2012, though the process by which these decisions are made and implemented is not known. Government officials justify such actions as necessary to "contain negative campaigns" on social networks. Google services, particularly its search engine and YouTube, also enjoy a high volume of user traffic. Despite its popularity, the BTRC blocked access to YouTube from September 2012 to early June 2013 after an offensive video clip, "The Innocence of Muslims," incited violent anti-American protests in Bangladesh, among other predominantly Muslim nations. Some critics said the length of the ban in Bangladesh indicates the disputed video was a pretext for officials to gain control over the video-sharing platform, which they have blocked in the past for politically sensitive content. However, in practice some ISPs informally unblocked the platform after just a few weeks. Other internet users continued to retrieve it using proxy servers or virtual private networks (VPNs) which allow internet users greater anonymity and access to blocked websites. So far, the BTRC has not sought to block these tools. According to the "Government Requests Report" of Facebook, at

25 Interviews with four industry experts in Bangladesh who requested anonymity, 2013.
26 Interviews with seven experts in Bangladesh who requested anonymity, 2013.
the second half of 2013, the social media site restricted access to three pieces of content reported by the Bangladeshi government under local laws, which prohibits criticism of the state.31

In December 2013, local news reports accused the Election Commission, an independent constitutional body of commissioners appointed by the president, of deliberately disrupting traffic to a contested section of its website. Since 2008, the commission has been required to publicize personal information about all candidates for parliamentary office, including personal assets. Anticorruption activists called for an investigation after newly-posted figures revealed many ruling party politicians had increased their wealth by more than 500 percent during their five years in power, and several news reports said an Awami League delegation asked the commission to withdraw the information.32 The following week, people reported that efforts to access the candidates’ affidavits were met with error messages; the rest of the site was unaffected. The Election Commission characterized the disruption as a technical error caused by overwhelming public interest, and the information was soon accessible again.33

Domestic websites, including the most popular news sites, Prothom Alo, BDNews24, and Banglanews24, are yet to face any targeted blocking. However, in March 2013, the government formed an official committee to identify bloggers who had allegedly demeaned the spirit of Islam.34 The committee participated in discussions with clerics to produce a list of bloggers and Facebook users they alleged had published anti-Islamic blasphemy.35 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 ultrareligious groups as well as the administration, which they accused of poor governance. They were subsequently arrested (see Violations of User Rights). The owners of the host platforms reported that officials never used court orders to support the action.36 At present, only Asif Mohiuddin’s account remains closed.37

Officially, the legal system ensures the right to appeal against most government decisions, but the lack of a warrant, as well as the risk of losing a license or legal permission to operate, makes mounting such an appeal challenging, and so far none 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. In particular, the Shahbag movement made discussion of religious issues more sensitive.

Major political parties significantly increased their online activity in the run-up to January elections, which were boycotted by the main opposition party, the Bangladesh Nationalist Party (BNP). The

36 Global Voices Advocacy, “Bangladesh Authorities Go After ‘Anti-Muslim’ Bloggers.”
37 Email interviews with Asif Mohiuddin, 2014.
incumbent Awami League had a dedicated new media team to reach out to voters. However, no commentators with undeclared sponsorship were documented manipulating online debate in favor of one side or the other.

Unknown actors have incited religious violence based on alleged Facebook activity. On November 2, 2013, a group in the Shanthia area of northern Pabna district accused a Hindu high school student of making anti-Islamic comments on a Facebook page, spurring attacks on the minority Hindu population. The boy’s family denied he was responsible for the page, which was photocopied and circulated, and the Daily Star newspaper said there was no evidence he was responsible for the content. Though unable to locate the boy, a mob beat his father, destroyed more than 25 local homes, and set fire to two temples before police subdued the crowd using teargas. In September 2012, members of the local Muslim majority community in southeastern Chittagong similarly accused a Buddhist of displaying an anti-Islamic image on his Facebook profile, and launched retaliatory attacks that destroyed a dozen temples. The Daily Star said the Facebook profile had been tampered with.

Despite recent restrictions and uncertainties, the number of active bloggers in Bangladesh is growing. The BTRC has identified 48 active domestic blog hosting platforms. Leading examples, based on subscriber figures, include SomewhereinBlog, Amarblog, and Shocholayoton. 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 the February 2013 war crimes tribunal verdict but 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 significant instances of online activism took place in Bangladesh, though groups in the capital, Dhaka, used digital tools to arrange protests against unpopular decisions made by the national cricket board and an affluent housing society management, garnering nationwide attention. In both cases the authorities gave in to popular demands, proving social media a viable tool for mass scale socio-political mobilization in Bangladesh.

44 Faheem Hussain, Zyma Islam, and Mashiat Mostafa, “Proliferation of Twitter for Political Microblogging in a Developing Country: An Exploratory Study of #Shahbag,” (unpublished research funded by the Asian University for Women Faculty Research Fund, 2013).
Violations of User Rights

In June 2013 Bangladesh saw its first sentence under the 2006 ICT Act, which prescribed harsh sentences for ill-defined categories of online expression, when a university lecturer was condemned in absentia to seven years’ imprisonment for threatening the prime minister on Facebook. In August, the authorities amended the act, making seven years the minimum possible jail term, while the maximum increased from 10 to 14 years. Police no longer need a warrant to make arrests under the act, and detained at least eight more internet users, human rights activists, and journalists for criticizing the government or offending Prime Minister Sheikh Hasina during the coverage period of this report. In September four bloggers who were the first people detained for violating the ICT Act in April 2013 were formally indicted for making allegedly anti-Islamic comments online.

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 legal reference for addressing issues related to internet usage, and defining as well as protecting freedom of expression online. 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 ($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 ($125,000).

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.

In 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. Before the amendment...
came into effect, police had to seek permission before making ICT-related arrests. Now no warrant is required, and offences under the act are non-bailable, meaning suspects must apply for bail at a court. The harsher provisions in the ICT Act may reflect the government’s insecurity regarding internet activism and security.

The amendment followed the first arrests ever made under the existing ICT act. In April 2013, as regulators were shutting down their websites, police detained bloggers Rasel Parvez, Masihur Rahman Biplob, and Subrata Ashikari Shuvo. Two days later they also detained Asif Mohiuddin, author of a renowned blog on sensitive sociopolitical issues that won a user-nominated award from German broadcaster Deutsche Welle in 2012. All four bloggers were charged with harming religious sentiment under Section 57(2) of the ICT Act 2006, and conservative political forces branded them as anti-Islamic atheists, though activists defended them. The first three bloggers were released on bail, but Asif Mohiuddin’s application was denied until he appealed on medical grounds in June. A judge declined to extend bail beyond one month; he was re-arrested and released again on bail later in the year. In September, all four were formally indicted. On February 16, 2014, the High Court of Bangladesh put the cases on hold for three months and asked the government to explain why those cases should not be scrapped. On March 2014, the High Court issued a stay order on Asif’s case until May 2014, which was later extended for a further period of six months.

Also in April 2013, police arrested Mahmudur Rahman, acting editor and majority owner of the pro-opposition newspaper *Amar Desh*, on charges that included defaming religion under ICT Act sections 56 and 57. The case was the latest in dozens of investigations involving Rahman that his supporters characterize as politically motivated. In 2012, he was charged with sedition in relation to his paper’s publication of private Skype communications involving a war crimes tribunal judge that

---


59 Email interview with Asif Mohiuddin’s legal counsel, July 2014.

cast doubt on the integrity of the tribunal’s judgments; the judge issued a court order against the United Kingdom-based Economist magazine in the same case, though much of the material was leaked online in Bangladesh. As of May 2014 he was jailed pending trial.

The year 2013 also saw the first sentence under the ICT Act. In June, a Dhaka court sentenced Hafizur Rahman Rana, a former Bangladesh University of Engineering and Technology lecturer who is now in hiding, to seven years in jail for threatening to kill Prime Minister Sheikh Hasina in an April 2012 Facebook post, based on a criminal complaint lodged by an Awami League political activist. The post compared Sheikh Hasina to a hyena. “I will shoot you [Hasina] in the head and in the stomach” as a warning to other hyenas, it said, according to news reports citing the prosecution. The court sentenced him in absentia to five years under Section 57 of the ICT Act and two years under the penal code for criminal intimidation. ICT law expert Tanjib-ul Alam told the national New Age daily that the sentence seemed harsh for a Facebook post and “may be perceived by general people as a sign of the government’s intolerance.”

At least eight more arrests were made in relation to online activity during the coverage period of this report.

In August 2013, police arrested Adilur Rahman Khan, secretary of the human rights organization Odhikar, and charged him under ICT Act Section 57 and Section 505 of the penal code. His bail petitions were rejected three times before he was released on October 11. Nasiruddin Elan, Odhikar’s director, was also named in the charge sheet, which accused Odhikar of “distorting images by using Photoshop and publishing a fabricated report, which enraged public sentiment” while documenting a government crackdown on protests in May. Elan surrendered to an arrest warrant in November and was later released on bail. In January they were charged under Section 57 of the ICT Act; the trial is ongoing.

In October 2013, the same political activist that complained against Hafizur Rahman Rana filed a defamation case against a National University geography lecturer A.K.M. Wahiduzzaman for

allegedly insulting Prime Minister Sheikh Hasina and her family on Facebook.\(^{70}\) After a month on bail, Wahiduzzaman was jailed on November 6 and obtained a year’s bail on November 24.\(^{71}\) On February 25, 2014, the high court issued a six-month stay order on the case. Meanwhile, the police filed another case against Wahiduzzaman under Section 57 of the ICT Act in March 2014.\(^{72}\)

On November 5, police in northern Mymensingh district arrested 28-year-old Shafiqul Islam Safiq for allegedly posting distorted pictures of Hasina and her father, Sheikh Mujibur Rahman, who is known as the founder of independent Bangladesh.\(^{73}\) On November 10, police in Dhaka arrested Md. Nurunnabi Shujan, a political activist from Jamaat-e-Islami’s student wing, for allegedly sharing and commenting on anti-Bangladesh content through Facebook.\(^{74}\) It is not clear if either individual was charged.

On January 16, 2014, police raided the Dhaka offices of national Bengali-language newspaper Daily Inqilab over a report investigating social media rumors that the Indian military helped quell pre-election violence in southwestern Satkhira district.\(^{75}\) The report was disputed by the Foreign Ministry. Rabiulla Robi, Inqilab’s news editor, Rafiq Mohammad, deputy chief reporter, and reporter Ahmmed Atiq were arrested and cases were filed against them under the ICT Act.\(^{76}\) The paper was temporarily shut down but continues to publish an online edition.\(^{77}\) On February 20, all three journalists were released on bail.\(^{78}\)

Separately, in April 2014, the war crimes tribunal initiated contempt proceedings under the ICT Act against a British journalist based in Bangladesh, for criticizing the court in blog articles published in 2011 and 2013.\(^{79}\)

There is no specific privacy or data protection law in Bangladesh. However, according to Article 43 of the country’s constitution, Bangladesh recognizes its citizens’ right to privacy and correspondence.\(^{80}\) The youth population has turned out to be the most vulnerable group against any privacy violations, predominantly through the voluntarily sharing of information via mobile phones and the internet.\(^{81}\)


\(^{72}\) Email interviews with AKM Wahiduzzaman, 2014.


\(^{80}\) Constitution of the People’s Republic of Bangladesh.

\(^{81}\) Faheem Hussain and Mohammad Sahid Ullah, “Mobile Communication and Internet in Bangladesh: Is Privacy at Risk for Youth Population?” Media Watch, Centre for Communication Studies, 2013.
People are slowly realizing the importance of protecting their online presence against any outside, unlawful intrusion.

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. While the BTRC uses deep-packet inspection to monitor for unlicensed Voice over Internet Protocol (VoIP) applications using granular online data, no abuse of this capacity for broader surveillance has been reported.

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.

Facebook reported it did not cooperate with government requests for information on 12 Facebook users in the first half of 2013. The government made seven more requests to Facebook during the period from January to June 2014, looking for information on 17 Facebook users, and Facebook rejected those requests as well.

Individuals have been subject to physical violence for online activity in Bangladesh. In March 2014, a mob attacked two teenagers in the city of Chittagong for allegedly posting blasphemous content on their personal Facebook accounts. Their attackers beat the two students in the street until police intervened, but the pair were subsequently arrested under the ICT Act and denied bail. One of the students wrote a blog and had criticized Jamaat-e-Islami and its student wing, and some bloggers speculated the blasphemy accusation came in retaliation for these comments or a personal enmity.

Bloggers were also violently targeted in 2013. Before blogger Asif Mohiuddin was detained later in the year, armed assailants hospitalized him in January 2013 with serious stab wounds. After his

---

Bangladesh

arrest, Mohiuddin reported verbal harassment from other prisoners and believes he remains on a hit list. In February 2013, leading Shahbag activist Ahmed Rajib Haider was brutally murdered by suspected religious extremists. 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. 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. The same group is accused of involvement with the attack on Asif Mohiuddin.

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.

---


Belarus

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Free</td>
<td></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>22</td>
<td>20</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>29</td>
<td>27</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>67</td>
<td>62</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 9.5 million

Internet Penetration 2013: 54 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Belarus experienced dynamic growth in internet access despite continued economic stagnation. In contrast to previous years, the government did not block access to social media platforms or communications apps (see Obstacles to Access).

- Diversity of online content is growing, and more Belarusians are using online sources of news and information (see Limits on Content).

- While there were fewer cases of prosecutions against internet users than in previous years, prosecutions and detentions continued and are likely to increase ahead of the presidential election in 2015 (see Violations of User Rights).
Introduction

The situation regarding internet freedom in Belarus was mixed in 2013-2014. The government, run by the autocratic president Alexander Lukashenka, moved to expand control over the online sphere in anticipation of presidential elections in 2015. There were fewer high-profile cases of prosecution against independent media as ongoing economic woes led the government to consider improving ties with the West. Additionally there were fewer instances of blocked websites, although harassment and detentions of activists for their online activities continued. One Belarusian media expert spoke of the government both “loosening and tightening the screws.”

Over the past year, the use of the internet continued to grow. In terms of ICT development, Belarus was the most dynamic country in the Commonwealth of Independent States (CIS) region during this period. The country’s external gateway capacity was expanded to 450 Gbps, the internet penetration rate continued to grow, and broadband access was the highest in the CIS region. All of Belarus’ mobile operators offer internet access, and the number of mobile internet users is growing. However, while access may be improving, the government continued to regulate, control, and restrict the scope of online content. Leading experts have found that Belarus continues to have one of the most restrictive media environments in Europe.

The authorities continued to administer a blacklist of websites whose access should be blocked in state-run facilities and cybercafes. The procedure for consigning sites to this secret list remains non-transparent and without an appeals process. As of February 2013, the last time the government acknowledged official figures, the list contained 119 websites, including some leading political, news, and human rights websites. At least 12 new sites were added to the blacklist in 2013-2014, although the actual number of sites to date remains unknown. The government continues to occasionally block certain independent websites under specific circumstances. In early 2014, for example, sites were blocked during the March 23 local elections and March 25 Freedom Day demonstrations.

In 2013-2014, there were about two dozen cases of detentions of online journalists, political and civic activists conducting online campaigns, and members of social networks. Instances of extralegal harassment of online activists, especially those involved in political communities on social networks, continued to take place. Meanwhile, the number of instances of technical attacks against independent websites fell in comparison to previous years.

Obstacles to Access

From 2013-2014, the number of internet users in Belarus continued to grow and the quality of internet connections improved, despite another year of economic stagnation. Continuing economic challenges did not dramatically affect government investment in the internet nor significantly increase internet costs, allowing more citizens to begin using the internet as a source of information and a tool for social interaction. The government’s inability to rebuild its popularity and restore its credibility after the 2010-2011 political and economic crises continued to spur demand for alterna-
Belarus

tive sources of information. With the authorities controlling all broadcast and most print outlets, the internet continues to serve as the country’s only island of independent media.

The Measuring the Information Society (MIS) 2013 Report of the International Telecommunication Union (ITU) found Belarus to be among the world’s most dynamic countries in terms of growth of household connectivity, households with a computer, households with internet access, and fixed and wireless broadband penetration. Belarus ranked 41st out of 157 countries on the ITU’s 2013 ICT development index, second only to Russia in the CIS region.

The National Statistical Committee reported that Belarus had an internet penetration rate of over 88 percent at the start of 2013, while an independent organization, Gemius, reported a penetration rate of 63 percent at the end of 2013. In contrast, the ITU placed the internet penetration rate lower at about 54 percent by the end of 2013, compared to nearly 47 percent in 2012 and just 23 percent in 2008. Still, a jump of over 7 percentage points in one year is significant. The National Statistical Committee noted that 97 percent of Belarusian companies and organizations and 48 percent of households had access to the internet in 2012. In 2014, almost 73 percent of Belarusian internet users visited social media sites.

The key divide in levels of access is not between rural and urban populations—since almost 75 percent of Belarusians live in urban areas—but between the country’s capital and other regions. However, the share of users in the capital city of Minsk has decreased from 40 percent six years ago to 28 percent as of November 2013, and internet users in other cities with a population of more than 50,000 now account for almost 20 percent of all internet users.

In November 2013, the country’s external internet gateway capacity was expanded to 450 Gbps, a growth of 80 percent capacity compared to a year earlier. By the end of 2013, Belarus’ wireless network had increased to some 50,000 hotspots, including over 6,000 in Minsk.

---

As of January 1, 2014, Belarus had over 11 million mobile telephone subscribers, 438,000 more than the year before, with a total penetration rate of nearly 120 percent. Belarus has three operators utilizing GSM; a fourth, which employed a CDMA network, ceased operating when the government cancelled its license for noncompliance in January 2014. At the beginning of 2014, the operators reported a total of 16,800 base stations covering over 98 percent of the country's area where nearly 100 percent of the population resides. All three mobile operators offer internet access; roughly one-third of all subscriptions are 3G-capable.

In 2012, almost 70 percent of Belarusian users reported having broadband access. This figure has increased rapidly since 2010, when Belarus had Europe's lowest level of high speed access, at only 10 percent of the population. Wireless use was up 26 percent in 2013 compared to the previous year. The largest selection and best quality of internet access is available in Minsk, where some 40 companies offer internet access through ADSL, ethernet, cable TV, and mobile networks. Smaller cities have a significantly narrower selection of options. Rural dwellers are largely dependent on the state-owned telecommunications company Beltelecom, which provides IPTV and internet access through ADSL (if phone lines are available), or via mobile internet, which is quite slow in remote locations. Internet connections are the slowest in the sparsely-populated areas of the southeastern and northern parts of the country.

The share of smartphones in the mobile market is approximately 40 percent. By October 2012, about 12 percent of internet users were accessing websites via mobile telephones, half of them with smartphones. According to one report, more than 2 million Belarusians have access to the internet via mobile devices, and more than 4 percent of online page views from Belarus now come from smartphones and tablets. More than 60 percent of Belarusian youth are reportedly using mobile internet.

---

11 “Total number of mobile telephone subscribers in the republic is over 11 million” [in Russian], Ministry of Communications and Informatization of the Republic of Belarus, January 24, 2014, http://www.mpt.gov.by/ru/content/2591. The ITU also placed the mobile phone penetration rate for Belarus at 118.8 percent by the end of 2013.
12 The operator was said to have failed to attain a population coverage of 90 percent. See “BelCel to lose wireless spectrum,” E-Belarus.org, January 14, 2014, http://www.e-belarus.org/news/201401171.html.
16 IPTV refers to “internet protocol over television”, a manner of providing television viewing through the internet rather than through traditional terrestrial, satellite, or other technologies.
17 “IT figures - statistics for Belarus” [in Russian], IT.tut.by, accessed January 27, 2013, http://it.tut.by/numbers/#cell. One of the three mobile phone operators, TeleGeography Mobile Digital Communications (Velcom), declared that as of December 31, 2012 its 3G/3G+ mobile networks were available to 100% of the urban population, while voice services coverage extended to 98.9% of the total population, E-Belarus.org, January 10, 2013, http://en.belapan.com/archive/2014/01/27/en_19290127H.
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 internet service providers. This makes it somewhat expensive to download large items like music or movies, while for common activities such as email and web browsing, the volume surcharges do not create a barrier for most users. An unlimited internet access service was launched by Beltelecom in 2007. Initially quite expensive, it has become more affordable: currently prices are approximately $5–$45 per month for individuals, depending on the speed. While mobile phone and internet access prices in Belarusan rubles increased several times in 2013–2014, the prices in dollars remained roughly the same due to Belarus’ chronic inflation.

According to Akamai Technologies, the average internet connection speed in Belarus was 2.6 Mbps in the third quarter of 2013. Belarus’s neighbors—Poland, Russia, and Ukraine—had average speeds ranging from 7.4 to 7.8 Mbps, while Latvia’s average was 11.1 Mbps. The global average was 3.6 Mbps, according to the same report. Ookla’s Household Download Net Index ranked Belarus 70th of 190 countries, with a download speed of 11.29 Mbps, in April 2014. One year earlier Belarus ranked 91st with average speeds of 5.46 Mbps. On average, Belarusian providers were selling 2 Mbps internet subscriptions without a traffic cap for around $10 per month. Such connections were more or less acceptable for comfortable web browsing, yet still slow for video streaming services like YouTube.

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 space. As a result, a particular feature of the Belarusan internet is its domination by portals, services, and social media sites based in neighboring Russia. Only two or three Belarusan sites are in the top 10 most popular internet sites in Belarus. Most Belarusan media consumers and internet users get their news and information in Russian from Russian websites. This situation became more problematic at the end of 2013 and the beginning of 2014 due to the Kremlin’s “information war” surrounding the Euromaidan protests in Ukraine and Russia’s occupation of Crimea. Most internet software used in Belarus is also in Russian, although some popular software is also available in Belarusan, often due to translation by local enthusiasts. In March 2014, the number of registered domain names in the Belarusan part of the internet (.by, often called the BYnet) exceeded 100,000, making it one of the top five fastest expanding domains.

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. Beltelecom, which was created in 1995, also holds a monopoly on fixed-line communications and internet services inside 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 and Information Technology has issued 180 licenses for secondary ISPs, though only about 60 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.

There is no independent regulator overseeing ICTs in Belarus. The Ministry of Communications and Information Technology handles regulatory functions. In addition, the presidential administration's Operations and Analysis Center (OAC) has the authority to oversee ISPs, conduct online surveillance, and manage Belarus' top-level domain (.by). Other bodies with authority over this sector include the State Telecommunications Inspectorate, State Control Committee, and Prosecutor General's Office.

Limits on Content

In 2013 and 2014, there were generally fewer attempts to limit content than there have been in previous years. With the general decline in repression against the independent media, including the dropping of criminal charges in several high-profile cases against internet users originally launched in 2012, there was also a decrease in self-censorship. The authorities continued to practice occasional blocking of certain independent websites with political, economic, or social content under specific circumstances. Because 2013 was not an election year, there was less blocking than during the previous year, when parliamentary elections took place. However, there was an uptick in blocking around the local elections on March 23, 2014 and on the March 25 "Freedom Day," a traditional day of protest for the country's democratic opposition.

The online human rights project conducted by Belarusian LGBT groups—Gaybelarus.by—has been blocked in Belarus, including from private computers and mobile phones, since June 2013. When accessed from Belarus, web browsers indicated that they could not connect to the website. At the same time, Gaybelarus.by is accessible in other countries. In August 2013, Alexievich.info, the official website of the internationally acclaimed Belarusian writer Svetlana Alexievich, who was nominated for the 2013 Nobel literature prize, was blocked. The website, hosted in Germany and available abroad, remains inaccessible in Belarus.

In October 2013, the leading independent trade union website Praca-by.info was blocked for three days. At that time the website was covering the hunger strike of independent trade union leaders at the state-run Mozyr Oil Refinery. The editor was contacted by a representative of the hosting com-

---


28 See “Instructions on the order domain names registration in the space of the hierarchical names of the national segment of the Internet network” at [http://cctld.by/eng/rules.html](http://cctld.by/eng/rules.html).

29 Unsuccessful attempts to access Gaybelarus.by from Belarus were made on June 8, 2013 and April 11, 2014. On the latter day, it was not accessible via Tor.

pany, who claimed that the website's account had been hacked, was distributing spam, and therefore had to be blocked by the provider while it conducted troubleshooting and identified the cause of the problem.\footnote{Trade union's website, reporting on the Mozyr hunger strike, is blocked [in Russian], Solidarnost i gazetaby.com, October 18, 2013, \url{http://gazetaby.com/cont/art.php?sn_nid=63085}.}

In March 2014, the webpages of a number of regional internet media, political parties and activists, and civil society leaders were hacked, presumably due to their coverage of or participation in local election campaigns.\footnote{Hackers and anonyms proliferate ahead of local elections, Belarusian Association of Journalists, March 21, 2014, \url{http://baj.by/en/node/24464}.} Several websites were blocked nationally as Belarusians went to the polls on March 23 to elect local government officials. The sites of the Belarusian Christian Democracy political party, the Tell the Truth civic movement, and the monitoring initiatives Right to Choose and “Election Observation: Theory and Practice” were inaccessible during parts of the election day.\footnote{Belarus Local Elections Update – March 23, Election Day 08:00-20:00, NDI Belarus Media Digest Special Edition, National Democratic Institute, March 23, 2014.} During the traditional Freedom Day demonstration on March 25, the live broadcast from Radio Free Europe/Radio Liberty's Belarusian service was blocked. The website of Nasha Niva (Nn.by), a leading independent media outlet, was also blocked during the protest march. The incident regarding Nn.by was the first time in which a blocked Belarusian website could not be accessed by the circumvention software Tor.\footnote{Online blocking in Belarus and how to fix it, Radio Svaboda, translated and posted by Belarusian Association of Journalists, March 26, 2014, \url{http://baj.by/en/node/24510}.}

The Lukashenka government has been blocking websites since the 2001 presidential election. To date, however, it does not appear to possess the capacity to employ sophisticated internet blocking techniques, and therefore resorts to more basic approaches like IP filtering and disabling DNS records.\footnote{In Belarus access to Change.org website is blocked [in Russian], Providers.by, August 13, 2012, \url{http://providers.by/2012/08/news/v-belarusi-zablokirovan-dostup-k-change-org}.} Also, it seems that the authorities do not perform regular or automated monitoring of the accessibility of banned sites, and it generally takes from 4 to 16 hours for a new IP address to be blocked. No documented instances of deep-packet inspection (DPI) filtering have been recorded so far.

Decree No. 60, which came into effect in July 2010, remains in force. The decree, which is designed “to protect the interests of citizens, society and the state in the information sphere,” introduced provisions by which ISPs are required to block access to restricted information, such as pornography and material inciting violence. By law, the authorities can only institute this blocking in state institutions or when requested by individual users. In practice, however, the government engages in ad hoc efforts to limit access to internet content deemed contrary to its interests, though Belarusian telecoms typically cite technical problems rather than admitting to blocking. The authorities have regularly blocked certain websites on specific days when there are elections, days symbolically important to the democratic opposition, or scheduled protests.

In June 2010, the Ministry of Telecommunications and the presidential administration’s Operations and Analysis Center (OAC) issued a regulation calling for the creation of two lists to catalog the URLs of all websites whose access should be blocked in state-run facilities and internet cafes; one list is
Belarus

public, while the other is accessible only to ISPs. As of May 2014, the publicly-accessible list did not contain any URLs, while the number of URLs on the restricted list remains unknown. According to Uladzimir Rabavolaw, the first deputy head of the OAC, the list contained 119 websites as of February 2013. The 2014 Report of the UN Special Rapporteur on the situation of human rights in Belarus suggests that 40 websites were blacklisted in 2013. At least 12 new sites, allegedly those advertising and promoting the use of narcotic and psychotropic drugs, were added to the blacklist in 2013-2014. The Prosecutor General’s office confirmed that two of the country’s most popular independent news and information websites, Charter97.org and Belaruspartisan.org, as well as the website of the Viasna Human Rights Center, Spring96.org, are on the restricted list. State bodies authorized to add sites to the blacklist include the Ministry of Internal Affairs, the Prosecutor General’s office, and the KGB.

The procedure for adding websites to the restricted list remains unclear and non-transparent. Civil society activists note that the government’s decisions are made arbitrarily, do not require judicial approval, and allow no course for appeal. After filing numerous complaints to identify the state body that made the decision to ban the Viasna website, the deputy chairman of the human rights organization received a reply from the Prosecutor General’s Office on December 10, 2013 (International Human Rights Day). The official letter stated that because Viasna was not registered by the Ministry of Justice, actions by an unregistered organization are punishable under Article 193.1 of the criminal code, and since Viasna’s website posted information promoting acts prohibited by law (i.e. acting on behalf of an unregistered NGO, organizing or participating in the activities of political parties religious organizations and foundations, which do not have official state registration), the Prosecutor General’s office had issued a decision to include this website in the list of those restricted in August 2011.

In response, Viasna’s board issued a statement stressing the legitimacy of the organization’s activities, which are guided by provisions of the Belarusian Constitution and international human rights standards ratified by Belarus. It also cited the UN Human Rights Committee’s Communication No. 1296/2004 of August 7, 2007, which found the decision of the Supreme Court to officially dissolve Viasna in November 2003 to be a violation of the right to freedom of association and recommended that the government reregister the organization. According to the OAC, the two popular indepen-

---

dent news websites, Charter97.org and Belaruspartisan.org, are on the blacklist because of alleged "copyright and journalism ethics violations."45

Under amendments dating from November 2011, which stipulate the fines for violating Decree No. 60, ISPs that provide access to blacklisted websites are required to pay a small fine. In practice, ISPs seem to be inconsistent in blocking access to these sites; some have blocked access to blacklisted sites without any user requests, which is technically illegal under the decree, while others have ignored the blacklist.46 ISPs block the blacklisted websites by web address or in combination with IP filtering. 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.47

Through its selective use of oppressive laws and threats, the government actively promotes self-censorship, which over the past few years has been a pervasive phenomenon for web-based media, especially state and commercial outlets. However, with the general decline in repression against online media, including the dropping of criminal charges in several high profile cases against online journalists and internet users originally launched in 2012, there has been a notable decrease in self-censorship over the past year. In the absence of acute social, political, or economic confrontations, Belarusian internet users generally felt safer in expressing their opinions online, despite the continued repression of critical journalism in print and broadcast media. Media experts have observed an increase in the quality and quantity of online discussions, including on social networks, offering anecdotal evidence to support the notion that people perceive the internet as a safer environment. This trend is also indirectly confirmed by the strong growth in the national (.by) internet domain, despite its more heavily regulated nature.

In December 2013, President Lukashenka issued a decree stating that his aide, Usevalad Yancheuski, would oversee and coordinate the operations of the country's television channels and news websites. Yancheuski, who is head of the Presidential Administration's Main Ideological Department, was directed to ensure that "government agencies and organizations conduct a single state policy in the spheres of information technology development, information and communication technologies, telecommunications and high technologies."48

Media experts and website moderators see trolling—the use of inflammatory, extraneous or provocative messages—as one of the government's less-direct methods of controlling the internet. Since the 2010-2011 protests, the number of trolls and paid commentators has significantly increased on independent websites, the blogs of civic activists and commentators, and popular opposition com-

As an increasing number of Belarusian internet users switch from forums 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, one can assume that there is some coordination behind their activities given the fact that they are constantly present on popular internet forums and social networks, immediately react to new developments, and frequently work in teams.\(^5\) In October 2013, the Ministry of Information refused a citizen’s request to act against trolls spreading false and malicious information on websites in his name.\(^5\)

Since 2008, the government has employed stringent requirements for accreditation to restrict non-state journalists’ access to information.\(^5\) The Law on Mass Media requires journalists to obtain authorization before they can become accredited, and it does not allow individuals to appeal the decision in cases where their accreditation is refused. Journalists, including those publishing online, are not allowed to work professionally if they are not accredited.\(^5\) There were multiple instances of warnings issued to non-accredited journalists, including those reporting online, in 2013–2014. In March 2014, for example, two Belarusian stringers working for the Poland-based Radio Racyja received a prosecutorial warning for their reporting and blogging on the station’s website, Racyja.com.\(^5\)

---


53 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. “Comments on Suggestions to Media Law,” Belarusian Association of Journalists, January 24, 2013, [http://baj.by/en/node/19255](http://baj.by/en/node/19255).


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.\(^{56}\)

The government continues to influence online content through significant financial support to pro-government media outlets, despite continuing economic woes. While the total amount of funding provided to progovernment online media is unknown, the 2014 state budget allocated €52 million ($71 million) in direct support for all state media, including €42 million ($57 million) to television and radio. Over €1.1 million ($1.5 million) alone was allocated to finance the internet portal of the president. These funds will be used to “collect, prepare and disseminate state orders on official information.”\(^{57}\) These sums are in addition to favorable advertising (70 percent of the economy is controlled by state-run companies), distribution contracts, and operating costs that are subsidized by the state such as preferential rent.

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 sites to be profitable. A series of restrictive amendments to the Law on Public Associations and the criminal code were passed secretly in October 2011 and came into force a month later. Of note were provisions that 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 grave threat to Belarusian independent media.\(^{58}\) Additionally, many independent online newspapers suffer from the negative financial impact of their print versions being regularly repressed and economically discriminated against.\(^{59}\)

Forced to operate in semi-underground conditions and facing constant pressure from the authorities, independent online media and opposition websites are unable to monetize their increasing audiences and growing popularity, despite the expansion of the market for online advertising. In 2013, Belarus’ internet advertising market increased by almost 50 percent over the previous year and reached about $10.5 million by the end of 2013, surpassing that of 2010 and indicating that the market had recovered from the financial crash of 2011. Experts predicted that online advertising would grow by 25 to 30 percent in 2014.\(^{60}\) Yet the share of internet advertising with regard to the total advertising market in Belarus remains one of the smallest in Europe.

---


\(^{60}\) “Internet advertising continues to lead the growth in the advertising market” [in Russian], January 31, 2014, http://marketing.by/main/市场/analytics/0065201.
Most independent news websites remain at an economic disadvantage because state and private companies are afraid to advertise on them. There is an unwritten rule advising state agencies and private companies not to advertise in the independent media, including internet outlets. When interviewed regarding the media market, one advertising executive said: “I have great respect for the independent media and what they are doing. But I don’t have a right to put at risk the interests of my clients and therefore I won’t place any serious amount of commercial advertising with independent newspapers or websites called the ‘fifth column’ by Belarusian authorities.” There were also cases when even foreign companies, especially those cooperating with state agencies, avoided placing ads on leading independent sites due to political concerns. As a result, even the most popular independent or opposition websites generate little or no advertising revenue.

The government continues its attempts to increase its own virtual presence and influence. In December 2013, the Minister of Information announced that a new portal bringing together the websites of all state-run (national, regional and local) newspapers would be launched under the aegis of the largest, progovernment daily newspaper SB-Belarus Segodnya. The editor of online projects at the paper confirmed that such a portal exists and is expected to start functioning in 2014.

Despite these and other efforts, government websites in general continue to underperform in comparison to their non-state peers. A 2013 independent review found that the websites of 45 government bodies did not comply with Belarusian law; not one met all the requirements regarding disclosure of information to the public. While the average site provided about 31 percent of the information required by law, the lowest performer, with a score of 12 percent, was the Operations and Analysis Center, the body tasked with policing Belarus’ internet.

The number of readers of print newspapers in Belarus is declining, and the government employs administrative controls and discriminatory economic measures to limit the growth of independent papers. As a result, the internet has emerged as the second-most popular mass media source of information, behind television, in Belarus. According to a mid-2013 survey, 63 percent of the population reported using the internet as a news source (including those who had heard about news items from friends or relatives who had read them online). Since 2010, in terms of audience growth, the best performing media in Belarus have been non-state online media. A majority of the country’s most popular news and information websites are either independent or opposition-run. According to the Belarusian ranking service Akavita.by, most of the top 20 and a majority of the top 50 news and information websites are run by independent or opposition groups, while the readership of state-controlled media sites has lagged behind. In terms of visits and page views, the readers of

---

independent online media are more loyal and consume more information than those of progovernmental websites.66

Social networks and blogs have also emerged as important sources of information. For example, a recent survey found that 24.3 percent of respondents had garnered information about developments in Ukraine from social media sites.67

According to the digital marketing agency Ashwood Creative, as of February 2014, 28 of the top 30 Belarusian media communities on Facebook were run by independent media and civil society groups.68 Recent comparative analysis of the media communities in 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.69 Progovernment sites have few readers, and state officials do not use social networks.70

Greater numbers of Belarusians are also reading independent news online because they find it more credible than the government’s version of developments in the country and abroad. A December 2013 survey found that more Belarusians trust independent media than the state media (41.1 versus 31.6 percent). Trust in the state media has dropped by 21.3 percent since December 2010. More than half of the population (55.3 percent) does not trust state media. Of the country’s 25 leading state and public institutions, non-state media ranked third in public trust, behind only the Orthodox Church and Army.71

Since the 2006 presidential election, independent websites, blogs, internet forums, and online communities have been playing a growing role in educating citizens, increasing voter turnout, monitoring the polls, and mobilizing protests against electoral irregularities. Beginning in 2010, social networks became an important tool for carrying out actions of solidarity and organizing 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 and 2012 parliamentary elections. Independent online media played an important role in documenting and reporting numerous violations committed by the state during the March 2014 local elections.

Belarus

The opposition’s dominance in the online media sector is proving alarming to the government, especially with presidential elections slated for 2015. As a result, the authorities appear to be moving to tighten control over the internet. As one media expert noted, the end of 2013 was “characterized by a more active persecution of internet-commentators and bloggers. These are still single cases, but it’s evident that the authorities are paying more attention to the Internet... It can be easily predicted that the closer the presidential election campaign, the stricter repression against social and political media we’ll observe.”72

Increasing internet penetration over the last several years has resulted in the continued growth of citizens’ activity on social networking sites. The Russian site VKontakte (vk.com) remains the most popular social network service; as of May 2013, it had 3 million accounts registered and was the most accessed website in the country.73 As of February 2014, more than 1.4 million Belarusians were using the Russian social network Odnoklassniki.ru.74 By contrast, the total number of Facebook users in Belarus was 900,000 by December 2013 (about 10 percent of the total population).75

In 2013, Belarusian civil society expanded its online activism in comparison to the year before. In one sense, this was a response to the rapid expansion of the internet and its active use by the opposition. But it was also the result of the government’s success in preempting most other forms of traditional, offline activism. In particular, online petitioning as a form of civic activism increased in 2013. More than 50 petitions addressing a gamut of issues were created and carried out by Belarusian rights groups and individuals on the Change.org platform alone. These online campaigns achieved varying degrees of success. When President Lukashenka floated the idea of an “exit tax” on Belarusians traveling abroad to shop, for example, or when his government suggested instituting a tax on the unemployed, civil society and media groups responded with strong online campaigns. An internet petition against the “exit tax” generated some 27,000 signatures. The online petitions were accompanied by a great deal of scorn and derision directed at the inane ideas, which dominated social networks. In the end, President Lukashenka was forced to publicly denounce the “exit tax” and the government abandoned both taxes. These online campaigns were, according to one observer, “the brightest examples of civic action in 2013.”76

Another tax, one on motor vehicles, did pass parliament, despite a similar online campaign which gathered more than 81,000 signatures in a matter of weeks. Through social networks and popular internet forums, activists attempted to organize offline protests against the new tax in December 2013. Although more than 100 cars and 200 pedestrians took part, police were able disperse the first protest in an hour. Participants were punished with fines and administrative arrests, an online community campaigning against the tax was deleted, and its administrator was briefly detained. On the eve of the second protest, related social network communities were invaded by trolls who worked

---

to persuade others not to take part in the protest. When checked, the personal pages of these commentators proved to be fake, with no updates, photos or followers. But the pressure succeeded; only about 10 vehicles took part in the second protest amid tight police security.77

In January 2014, some 4,000 people signed an online petition calling on President Lukashenka and the Minister of Health to at least double the pay and improve the working conditions of emergency medical service providers. While the government pressured the initiators to withdraw the petition and put one of them on unpaid leave, it also agreed to a pay raise for ambulance workers.78

Violations of User Rights

In 2013-2014, prosecutions against internet users decreased, though harassment and detentions continued. According to Viasna, there were more than 50 cases of politically-motivated administrative persecution (arrests, detentions, and fines) documented in 2013, but this was significantly fewer than the 233 recorded in 2012.79 The Belarusian Association of Journalists registered approximately 50 cases of detentions of journalists (including online and offline journalists), independent press distributors, and members of social networks by different law-enforcement bodies in 2013, a decrease of 20 cases in comparison to the year before. Detained media practitioners were usually released within a few hours.

While the rights to freedom of expression and information are guaranteed by the Belarusian constitution, they remain severely restricted and violated in practice. Formally, there are no laws ascribing criminal penalties or civil liabilities specifically for online activities, but since 2007, the government has employed a series of repressive laws—mainly defamation laws—that target traditional media to stifle critical voices online.

In October 2011, the parliament approved an “anti-revolutionary” package of amendments to laws regulating civic organizations and political parties, as well as to the criminal code. These amendments—which also apply to internet-based media outlets—further criminalize protest actions, make receiving foreign funding a criminal offense, and extend the authority of the KGB. Under the amendments, the KGB is freed from the oversight of other state bodies and was given powers that were previously granted only during a state of emergency, including the right to enter the homes and offices of any citizen at any time without a court order.80

In 2013, there were several cases of the government prosecuting online users for critical comments on the internet, though fewer than in previous years. In July 2013, Andrei Karelin was found guilty of offending a police officer and fined $1,050 for two critical comments he had posted on an internet forum a few months earlier. The comments reflected negatively on the Belarusian police and their

Belarus

professionalism, and declared that “all normal citizens” hate them. The case was monitored personally by the Minister of the Interior Ihar Shunevich. In August, Mr. Karelin was forced to quit his job as a playwright at a drama theater. He has launched his own crowdfunding website to pay the fines.81

The authorities continue to detain and prosecute citizen journalists and bloggers for their watchdog activities. In July 2013, Ruslan Mirzoeu, a Minsk worker (and a former drug user on parole), became a BYnet celebrity after shooting a series of clips about everyday life at his factory and posting them on YouTube. Full of black humour and inconvenient insights about one of Belarus’ leading industries, his “Chronicles of the Plant” videos were reposted by leading independent websites and viewed by hundreds of thousands online. In July, he was fired from his job at the Minsk Automobile Plant (MAZ). In August, he released two new films representing urban life in one of Minsk’s suburbs, including depictions of poverty, drug addicts, alcoholics, and prostitutes. He was arrested, tried for using curse words “in public” in the videos, and sentenced to seven days in prison for hooliganism. An official commented on the evening news that the case was not about using crude language but punishing someone for becoming popular by “manipulating social problems.”82 In September, district police in Minsk brought a criminal case against Mr. Mirzoeu for violating his parole. On December 13, he was sentenced to one year in prison.83

In October 2013, Aleh Zhalnou, a well-known blogger in Bobruisk who exposes instances of illegal police actions, was arrested with his son for allegedly attacking traffic police. Zhalnou claims that he and his son were the victims of police retaliation after some 2012 incidents in which he allegedly slandered the police and a September 2013 incident in which he filmed police being unresponsive to a complaint and posted the evidence online. Zhalnou was forced to undergo a psychiatric exam and was unable to update his webpage after the raid. In February 2014, he was detained again and questioned by the police for 12 hours on suspicion of planning a bombing. During both arrests, the police confiscated his computer and electronic equipment. A criminal case was launched against him for allegedly insulting the police through online posts. In March 2014, Zhalnou was fined for posting on his YouTube channel a video recording of a meeting he had with a police official.84

In December 2013, several activists were detained in connection with the “Stop Tax” online campaign against a new tax on vehicles (see Limits on Content). Police in Mogilev demanded that Anton Kastou, a political activist and member of the “Stop Tax” online campaign, delete the “Stop Fear” site from social networks. After the “Stop Tax” group discussed the possibility of holding a protest on the social network VKontakte, Kastou was sentenced to three days in jail for “organizing and holding


Belarus

a mass event." His laptop was confiscated. Dzmitry Paliyenka, a political activist and the alleged administrator of the "Stop Tax" social network in VKontakte, was jailed for 15 days for alleged "disorderly conduct." It is important to note that these crackdowns were ostensibly of a preventative nature as they took place before the scheduled protests were carried out. Other activists involved with the "Stop Tax" campaign were also fined or briefly jailed for their online calls for protests against the tax.

The government also levied fines for "online picketing" to stifle Belarusians’ attempts to express solidarity with their Ukrainian neighbors protesting in Kyiv. In February 2014, at least two fans of the Belarusian soccer champion team BATE Borisov were jailed for up to five days for participating in an unauthorized mass event. The individuals had allegedly posed with other fans for a photograph with an opposition flag and banners displaying solidarity with Ukrainian anti-government protesters, which was then posted on the internet. The faces of the some two dozen fans in the photo had been blurred out. In April, three activists were fined for having photos taken of themselves with Belarusian and Ukrainian symbols in historic places and posted on the internet.

These incidents demonstrate several important trends in 2013-2014. Experts point to a new type of repression against online activists, particularly those focused on holding officials accountable. Rather than blocking individual sites, the government is punishing citizen journalists and activists for their online activities. Observers noted that the government has adopted the same strategy of targeted repression that has proved effective in suppressing dissent in other civic and media sectors. And it is increasingly doing this by taking laws originally designed to limit traditional activism and applying them to online cases. As the 2014 Report of the UN Special Rapporteur on the Situation of Human Rights in Belarus noted, "The online media continued to be severely affected by a new trend of applying extra-journalistic regulations to web activities."

Another trend that has become prominent is the government's use of materials obtained online as "evidence" to punish individuals for alleged offline crimes or misdemeanors. Additionally, while most cases of prosecution in 2012 were based in Minsk or larger cities, a majority of the 2013 cases took place in the country's regions. This is partially due to the rise in the quantity, quality, and impact of independent regional online media.

87 "BATE fan: ‘At the police station I was shown a photo and told that I was in it;’" Viasna, February 4, 2014, http://spring96.org/en/news/68863.
Since Belarusian users have regular access to most online resources under normal circumstances—as blacklisted sites are blocked only in public facilities, not private offices or households—users generally have not employed proxy servers or other circumvention tools, leaving them vulnerable during politically sensitive periods when targeted disruptions occur. Circumvention tools have not been blocked by the authorities. Most often, people are reminded about blocking, hacking, trolling, and phishing only when it takes place.92

Individuals are still required to present their passports and register when they buy a SIM card and obtain a mobile phone number. All telecommunication operators are obliged to install real-time surveillance hardware, 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 (such as user history, account balance, and other details) without judicial or other oversight. Mobile phone companies are required to turn over personal data of their customers at the government’s request.

Since 2010, the Belarusian government has allocated resources for online surveillance technologies.93 In 2012, there were reports of Western firms supplying telecommunications hardware and software that would allow the state to expand its surveillance of citizens.94 Russian surveillance technologies, including SORM (System for Operative Investigative Measures, an electronic intercept system) are also employed by the Belarusian government.95 Decree No. 60 requires ISPs to maintain records of the traffic of all internet protocol (IP) addresses, including those at home and at work, for one year. As a result, the state can request information about any citizen’s use of the internet.

The authorities claim that the protection of personal data is a priority. On July 26, 2013, the Law on the Population Register finally came into force after delays caused by the 2011 financial crisis. The register, which is aimed at making information exchange between state agencies more efficient, is a central database that contains the personal data of all Belarusian citizens, including name, gender, personal identity number, date and place of birth, a digital photo, marital status, employment and education, tax obligations, etc.96 In order to avoid any leaks of personal data, the register is being created on internal networks of the Ministry of Internal Affairs. While similar registers exist in more than 60 countries, independent Belarusian experts are concerned due to the repressive nature of the Ministry and because Belarus remains the only post-Soviet state that has no proper legislation regulating the protection of personal data; the country also has not joined the Convention of the Council of Europe “For the Protection of Individuals with regard to Automatic Processing of Personal Data.” Moreover, the Law on the Population Register does not allow citizens to obtain information about which state agencies are viewing their personal data.97 In general, independent experts conclude

---

that “Belarusian legislation does not provide satisfactory basis for the proper balance between freedom and security online.”

As of 2007, internet cafes are obliged to keep a year-long history of the domain names accessed by users and inform law enforcement bodies of suspected legal violations. In December 2012, the Council of Ministers abolished the requirement that customers must present their passports at internet cafes. Instead, employees are now required to take pictures of or film visitors. Meanwhile, restaurants, cafes, hotels, and other entities are obliged to register users before providing them with wireless access, whether free of charge or paid.

In the absence of elections and other major socio-political events in 2013, there were fewer recorded instances of extralegal intimidation and harassment for online activities on social networks than in previous years, though this was still a prominent trend.

Over the course of 2012-2013, Ihar Pastnou, a psychiatrist at the Vitebsk Center for Narcology and Psychiatry, posted a series of videos on YouTube that were critical of the health care system in Vitebsk. In particular, he highlighted medical errors, mismanagement, and misuse of funds by the head of the regional government. On August 16, 2013, Dr. Pastnou was forcibly taken to the psychiatric ward at his place of work for treatment. On August 23, a Vitebsk District Court ordered that he attend compulsory psychiatric treatment. Dr. Pastnou was diagnosed with “psychopathic personality disorder with a mania for persecuting the authorities,” kept in isolation, and banned from having any visits, correspondence, or telephone calls. On September 30, Dr. Pastnou was discharged from the hospital, but is required to visit a psychiatrist regularly. He has demanded an independent examination, considers his case to be an example of punitive psychiatry, and is appealing to the Supreme Court. Dr. Pastnou’s case will be considered by the UN Human Rights Committee.

On December 24, 2013, police searched the apartment of Anton Kastsou, a member of the United Civic Party in Mahiliou. The police demanded that he remove the “Stop Fear” community from the VKontakte site, despite the fact that the activist had written a statement denying he was a creator of this community, though he agreed to delete his own comments from the group. The “Stop Fear” community was created in order to organize weekly protests against a proposed motor vehicle tax (see Limits on Content).

---

101 Including the user’s name, surname, type of ID, ID number, and name of the state body which issued the ID, as per Article 6 of the Regulation on computer clubs and internet cafe functioning, http://pravo.by/main.aspx?guid=38718p0=C20700175&n2= (NRPA).
In June 2013, Siarhej Androsenka, the leader of the online human rights project conducted by Belarusian LGBT groups—Gaybelarus.by—left the country following a long campaign of persecution and psychological pressure against him and his family by Belarusian law enforcement agencies.105

In August 2013, police raided the apartment of Henadz Zhuleba, a blogger in Svetlahorsk, and confiscated his computer after he had posted a video online spotlighting the luxury home of the head of the local administration. The official’s wife complained about the clip and accused him of libel. The police told the activist that they would examine the files on his computer before deciding whether to launch criminal proceedings against him. Earlier, the blogger had posted other critical videos online showing the poor state of roads and other social infrastructure in his town.106

In November 2013, the apartment of Dzianis Dashkevich, the editor-in-chief of the website Vorgachev.ru in Rahachau, was searched and two computers were confiscated. The inspection was based on a criminal case related to allegations of insulting a local official. The activist and his independent website had previously received official warnings regarding the publishing of “inaccurate information about the political and economic situation in the country.”107

In January 2014, an online petition designed to increase salaries and secure better working conditions for the workers of Belarus’ emergency medical services, appeared on Change.org and collected over 5,000 signatures, including those of thousands of medical professionals, in less than two days. But after this period, the initiator, Aliaksei Ipatau, announced that the petition had to be withdrawn without any explanation.108 The petition was removed from the website, presumably due to government pressure. Another organizer of the campaign, Vital Aheyenka, was forced to take unpaid leave from his ambulance job.109

There were some instances of technical attacks against the websites of independent media and civil society groups during the coverage period. On April 25, 2013, the websites of Belarus Partisan (Belaruspartisan.org) and the Viasna Human Rights Center (Spring96.org) were hacked. Threatening messages were left on the sites, calling them “traitors” and “slanderers” of the Belarusian people.110 Both sites are on the government’s list of web resources banned at state institutions.

On December 8, 2013, the websites of the Belarusian, Ukrainian and other services of Radio Free Europe/Radio Liberty (RFE/RL) were unavailable following a massive DDoS attack. Cyberattacks against RFE/RL have occasionally occurred since the beginning of mass protests in Ukraine in November.111

108 “Signature collection of the ambulance workers for an appeal to Lukashenka was forcibly stopped” [in Russian], January 8, 2014, Radio Svaboda, http://www.svaboda.org/content/article/25223456.html.
Belarus

On December 18, 2013, the leaders of Belarus’ largest civic campaign “Budzma” (“Let’s be Belarusians”) distributed a statement reporting that they had lost access to the campaign’s website domain Budzma.org and its administrative system, and asked all users to switch to a reserve website at Budzma.by. The causes of the problems are being investigated by “Budzma” leadership.112

Belarusian criminal law prohibits these types of technical violence. Specifically, Article 351 of the Criminal Code, covering “computer sabotage,” stipulates that the premeditated destruction, blocking, or disabling of computer information, programs, or equipment is punishable by fines, professional sanctions, and up to five years in prison.113 A special department at the Ministry of Internal Affairs is tasked with investigating such crimes. In reality, a number of the attacks on the independent websites and personal accounts of opposition activists have been linked to the authorities. The government has stated its intention to accede to the Council of Europe’s Convention on Cybercrime, but it has made no move to sign on to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.114

Brazil

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free</td>
<td></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>8</td>
<td>7</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>17</td>
<td>16</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>32</td>
<td>30</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 195 million

Internet Penetration 2013: 52 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: No

Bloggers/ICT Users Arrested: No

Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- In December 2013, President Dilma Rousseff issued a decree exempting certain categories of smartphone from taxation. Included were those with national content, Wi-Fi connectivity, email access, and open source code (see Obstacles to Access).

- In April 2014, Brazil’s highly anticipated Marco Civil Bill, a so-called “Constitution for the Internet,” was signed into law, ensuring privacy protection for users, net neutrality, and several other positive measures (see Violations of User Rights).

- In September 2013, the Superior Electoral Court authorized the use of Twitter during electoral campaigns, while amendments to Brazil’s electoral law in December 2013 established additional restrictions to online publishing of electoral content, as well as fines for potential violators (see Violations of User Rights).

- Beginning in April 2014, cyberattacks against Brazilian government websites and infrastructure increased markedly ahead of the FIFA World Cup games (see Violations of User Rights).

- Social media played a key role in the June 2013 Free Fare Movement, both as a tool for mobilizing protestors (see Limits on Content) and as a means of documenting abuse of reporters covering the protests (see Violations of User Rights).
Introduction

After years of debate and revision, Brazil's highly discussed Marco Civil da Internet bill, hailed as a civil rights framework for the internet, was approved by the lower house of Congress in March 2014, without onerous requirements related to localization of data storage. The final text of the Marco Civil—which was approved by the Senate and signed into law by the president in April—also contains key provisions governing net neutrality and ensuring strong privacy protections, and further touches on regulation for intermediary liability. The Marco Civil law has received significant international attention as a new type of legislation predicated on ensuring individuals' rights as they pertain to the internet.

Brazil, which was first connected to the internet in 1990, 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 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. 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 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, and public health. In some cases, such as the Free Fare Movement, online debate has catalyzed real-world protests.

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 proceedings before domestic courts and governmental bodies. Reporters Without Borders no longer ranks Brazil as among the world's five deadliest countries for media personnel.1 Five journalists were assassinated in 2013, representing a continuation of the previous year's trend; however, retaliatory violence against journalists and bloggers does appear to be on a decline.

Additionally, Brazil's Electoral Act—which faced criticism for broad language that posed a threat to freedom of speech—was amended in September 2013 to establish the use of Twitter as an acceptable medium in political campaigning. The Act was amended again in December 2013, however, with additional restrictions to online content concerning candidates and political parties.2

---


2 Presidency of the Republic, Civil House for Legal Affairs, Law No. 12.891 of 2013, [http://www.planalto.gov.br/ccivil_03/Ato2011-2014/2013/Ley/L12891.htm#art3](http://www.planalto.gov.br/ccivil_03/Ato2011-2014/2013/Ley/L12891.htm#art3)
Obstacles to Access

According to the most recent figures from the International Telecommunication Union (ITU), despite its burgeoning economy, Brazil’s internet penetration rate remains below the average for North American and European countries.3 According to the International Telecommunication Union (ITU), Brazil’s internet penetration rate increased from 49 percent in 2012 to 52 percent in 2013.4 Almost 60 percent of Brazilian residences lack internet access; a reality resulting from various obstacles, such as high prices—a problem that extends to fixed broadband, wireless, and 3G/4G technologies—limited availability of services, and persistent social inequalities.5

The 2013 Web Index ranks Brazil 33rd globally in terms of internet access, freedom, openness, relevant content, and empowerment; Chile, Mexico, and Uruguay are all ranked higher regionally.6 Internet penetration varies greatly in Brazil, with noteworthy infrastructural disparities evident between various geographical regions, as well as between urban and rural areas.

Fixed broadband technology, such as DSL and cable, accounts for 68 percent of household internet connections in Brazil.7 Although mobile broadband is still in the minority with 18 percent of the market, such technology now accounts for most new household broadband connections, indicating that Brazil is following global broadband growth trends. As of the third quarter of 2013, Akamai measured Brazil’s average internet connection speed at 2.6 Mbps.8 According to figures published by the ITU, over 20 million Brazilians have fixed-broadband connections,9 22 percent of which are high speed, 26 percent of which are medium speed; the remaining 52 percent are low speed.10

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 nearly 68 percent of those from the lowest economic brackets.11 Although household access is becoming the

---

5 Cetic.br, Coordination for ICT strategies, “No Brasil, 60% das Casas Ainda não Yêm Internet” [In Brazil, 60 Percent of Households Still do not Have Internet], Cetic.br, July 1, 2013, http://coeti.seplag.ce.gov.br/?m=20130701
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.12

Internet growth has been slower than expected in Brazil, yet mobile penetration has grown significantly over the past five years, increasing by an average of 19 percent annually and reaching 134 percent by the end of 2013.13 As of January 2014, there were 271 million mobile phone subscriptions in Brazil, an increase of 3.5 percent from 2013. Smartphone sales increased significantly in 2013 as well, growing by 147 percent,14 a figure consistent with the country’s recent expansion of mobile broadband access. As of December 2013, 103 million Brazilians had mobile broadband access, suggesting an increase of nearly 42 percent as compared to November 2012.15

Nearly 95 million users (approximately 35 percent) now have 3G service16 and over one million utilize 4G technology.17 Such advanced connections are so heavily concentrated in São Paulo that if the city itself were considered a country it would be the fifth largest market in Latin America.18

The development of mobile technologies supporting 4G services was greatly hastened by the anticipated demand leading up to and during the June to July 2014 World Cup. While national wireless networks are still small compared to other countries—as of December 2013, the National Agency of Telecommunications (ANATEL) had registered approximately 160,000 hotspots within Brazilian territory19—mobile service providers were working to increase the number in the first half of 2014 as a means of accommodating anticipated increases in 3G/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.20

---

19 Globo, “Operatoras Ampliam Pontos de Wi-Fi para Desafogar Rede 3G e 4G” [Mobile Companies Expand Wi-Fi Hotspots to Ease 3G and 4G Networks], Globo, January 16, 2014, http://oglobo.globo.com/tecnologia/operatoras-ampliam-pontos-de-wi-fi-para-desafogar-rede-3g-4g-11323040#ixzz2HID00EFH.
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) aims to triple broadband access by the end of 2014.\(^{21}\) According to statistics from the Brazilian Telecommunications Association, nearly 134 million internet connections were facilitated by broadband in 2013, suggesting an increase of 55 percent for that year.\(^{22}\) Another initiative concerns the Special Taxation Regime of the National Broadband Program (Tributação do Programa Nacional de Banda Larga, or REPNBL), a new framework establishing tax incentives for the ICT sector, which was passed in February 2013. REPNBL complements the 2010 National Broadband Plan (PNBL) and is intended to encourage investment in existing telecommunications networks in order to expand and modernize broadband and mobile internet capabilities.

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/4G technology. In December 2013, President Rousseff issued Decree No. 7,981/2013, which amended a portion of REPNBL 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.\(^{23}\)

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 indications that Brazilian authorities 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. E-commerce has also been growing in recent years, with 20 percent of online payments conducted by smartphones or tablets in 2013.\(^{24}\) Economists expect e-commerce in Brazil to grow nearly 12 percent in 2014, reaching US$13 billion by year’s end.\(^{25}\)

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 characterized by high concentration. As of December 2013, the market share of four companies—Oi, NET, Telefonica, and GVT—corresponded to almost 90 percent of the country’s broadband market.\(^{26}\) In January 2014, the Brazilian antitrust authorities approved the merger of Oi and Portugal Telecom into CorpCo, which ranks as the leading telecommunication company in Brazil and in Portuguese-speaking countries.


\(^{25}\) EMarketer, “Retail Ecommerce Sales in Brazil to See Double-Digit Growth This Year,” EMarketer, January 24, 2014, [http://www.emarketer.com/Article/Retail-Ecommerce-Sales-Brazil-See-Double-Digit-Growth-This-Year/1010556](http://www.emarketer.com/Article/Retail-Ecommerce-Sales-Brazil-See-Double-Digit-Growth-This-Year/1010556).

worldwide.\footnote{27} Recent data regarding Brazil's mobile market indicates that four large 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.\footnote{28} Such high market concentration could make it very difficult for other providers such as CBTC and Nextel to compete in the mobile sector.\footnote{29} Despite such concentration, Brazil's mobile industry has been booming, and appears to be the largest such market in Latin America.\footnote{30}

Two regulatory agencies oversee Brazilian ICTs: ANATEL, viewed by some Brazilians as inefficient and relatively slow, and the Administrative Council for Economic Defense (CADE), an antitrust body that is perceived as more effective in addressing merger reviews and anticompetitive practices in telecommunications markets. While both agencies 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.\footnote{31} 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.\footnote{32}

The Brazilian Internet Steering Committee (CGI), a multi-stakeholder organization created in 1995, plays a substantive role in Brazilian internet governance and regulation debate, and was particularly influential in the June 2009 adoption of the “Principles for the Governance and Use of the Internet”—which include the goals of online freedom, privacy, human rights, and net neutrality.\footnote{33} In May 2013, the Committee announced its intention to expand its policymaking activities in these areas.\footnote{34} CGI's contributions include comprehensive and reliable annual reports on the status of internet adoption in Brazil, as well as funding for internet governance-related research and academic publications. Committee members are elected from the government, the private sector, academia, and nongovernmental organizations. The latest group of delegates was chosen in 2010 in relatively

\footnote{27} Reuters, “Brazil Competition Watchdog Approves Oi, Portugal Telecom Merger,” January 14, 2014, \url{http://www.reuters.com/article/2014/01/14/oi-portugaltelecom-cade-idUSL2N0KO0HO20140114}.
\footnote{33} CGI.br, Principles for the Governance and Use of the Internet, accessed February 13, 2014, \url{http://www.cgi.br/english/regulations/resolution2009-003.htm}.
\footnote{34} For more information on the activities of the Brazilian Internet Steering Committee, see the official website of CGI.br, \url{http://www.cgi.br}. 

---

Brazil
democratic and open elections. The most recent elections, which were largely viewed to be free and fair, were concluded in early April 2014.

**Limits on Content**

Brazilians’ use of social media tools for civic action and activism significantly expanded over the past year. 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 indications that Brazilian authorities are filtering or blocking 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 and disputes related to intermediary liability continue to pose significant challenges in Brazil, affecting social media activity, social networking providers such as Google and Twitter, and video-sharing websites such as YouTube, a notice-and-takedown provision in Brazil’s newly passed Marco Civil da Internet law is intended to clarify the situation.

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. As of November 2013, over 60 million Brazilians had Facebook accounts. This figure, which represents one third of all Latin American Facebook users, has been growing at a rate of approximately 15 percent annually, placing Brazil just behind the United States and India in terms of Facebook adoption rates. Brazil is also home to the fifth largest contingent of Twitter users in the world; among non-English speaking countries, it is tied with Spain for the highest percentage of users.

According to the Google’s Transparency Report, between January and June 2013, Brazil issued 237 court orders and 84 executive requests to remove content, the majority of which cited defamation or privacy and security concerns. There were 10 executive requests and 13 court orders for the removal of material that allegedly infringed upon electoral law. One such court order called for the removal of 107 blog posts and search results related to allegations of corruption in a public procurement process in which a candidate was criticized. Google also received court orders to remove 68 blog posts accusing a local judge of corruption and 220 blog posts that criticized a city

---

A small portion of cases also pertain to infringement of copyright, nudity, and incitement to hate and violence. Although Brazilian requests for content removal issued to Google have been hovering at a steady level over recent years, those issued to Twitter are declining. With the exception of emergency situations or legal prohibitions related to a specific case, Twitter notifies users of requests for account information.

State-initiated censorship continues to be an ongoing trend in Brazil in the context of electoral disputes. Many such instances deal with defamation and result in the imposition of fines and the removal of content related to elected officials. The Electoral Act of 1997 has been under intense congressional revision, court scrutiny, and public debate, particularly because its broad terms harbor the potential to constrain freedom of expression both online and offline. The electoral law—which restricts content that could be viewed as injurious to a candidate, prohibiting such material from publication for three months prior to election day—once pertained primarily to offline materials; however, 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. Journalists and bloggers who disregard the directive are subject to fines and potentially even prison sentences, and numerous articles or posts are often implicated in removal requests issued by electoral courts for material which may infringe upon the law.

Despite the broad restrictions on content inherent in the Electoral Act, in September 2013, the Superior Electoral Court authorized the use of Twitter during electoral campaigns. The leading opinion stated that messages exchanged between Twitter users are restricted to those who wish to receive the information; accordingly, it was decided that Twitter does not fall into the category of mass media (which includes radio and television). In December 2013, however, the Brazilian National Congress passed a new amendment to the Electoral Act (Law No. 9.054/97), establishing additional restrictions to online publishing of electoral content, as well as fines for potential violators. Such restrictions include: liability of servers with regard to early online campaigning; unsubscribing mechanisms of 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. Given that the amendment was approved less than a year before the 2014 elections, legal controversy has surrounded the scope of its application. Although the effects of these recent changes to electoral

---


laws remain to be seen, Brazil will likely witness the impact of new legislation beginning in late summer of 2014, as presidential elections are slated for October.

Intermediary liability has been a highly visible issue in Brazil. Social networking platforms such as Facebook and Orkut (owned by Google) have been involved in intermediary liability disputes and are the main target of civil liability claims regarding content removal and defamation. State courts have largely been divided on the issue of intermediary liability, however, with some attributing the legal burden directly to the intermediary, and others adopting notice-and-takedown approaches that impose liability only if an intermediary fails to remove content after judicial notice. In late 2013 and early 2014, however, the Brazilian Superior Court of Justice (STJ) issued several decisions on the matter. In most cases, it ruled that while ISPs are not responsible for prescreening content, they are liable for complying with court-issued notice-and-takedown requests within 24 hours. Failure to fulfill this requirement can result in fines and damages. Accordingly, in a September 2013 case, the STJ issued a decision imposing fines on Google for not immediately complying with an order to remove content. Similar decisions have confirmed the notice-and-takedown procedure, which was likewise strengthened by the 2014 passage of the Marco Civil da Internet legislation. The Marco Civil law creates a “safe harbor” for intermediaries via the official establishment of a judicial notice-and-takedown framework. Due to its emphasis on clarifying previously murky legal questions concerning intermediary liability, this provision should also prevent pre-emptive censorship by parties uncertain about their legal obligations.

Standards of access to public information in Brazil have evolved in recent years, particularly since the November 2011 enactment of the Access to Public Information Law (No. 12.527/2011). Among the main goals of the statute are to achieve greater transparency at the governmental level, to optimize civic participation and social action, and to allow the exposure of corrupt practices at the federal, state, and municipal levels. Citizens are also entitled to request governmental information via the internet. In this vein, state bodies are working to adopt online platforms for the disclosure of information relating to public administration, governmental procurements, projects, and finances. Such information must be disclosed in a user-friendly, accessible, and current manner, enabling community access free of technical barriers.

One key mechanism of the Access to Public Information Law is the Electronic Information System Service to the Citizen (e-SIC), which allows any individual or legal entity to submit a request to

---

47 Brazilian Superior Court of Justice (STJ), Appeal to the Superior Court No. 1338214 / MT (November 21, 2013); See also: Brazilian Superior Court of Justice (STJ), Appeal to the Superior Court No. 1407271 / SP (November 21, 2013).
governmental bodies or entities of the Federal Executive Branch for access to public information.\(^{53}\) As of December 2012, the Federal Government had received 55,000 requests for information, most of which were addressed to regulatory agencies and publicly held companies.\(^{54}\)

Brazil is also a founding member of the Open Government Partnership (OGP)—a global effort to increase government transparency, efficacy, and accountability.\(^{55}\) According to a recent OGP report, to date, Brazil has secured 32 commitments by 5 governmental bodies, 18 of which have already been completed.\(^{56}\) Another OGP report states that the Brazilian Open Data Portal (Portal Brasileiro de Dados Abertos) has published 82 sets of data and approximately 1,000 resources.\(^{57}\) Its institutional goal is to be the main reference for public searches and access to governmental data in Brazil.\(^{58}\)

Social media platforms such as Facebook and Twitter are increasingly used for civic activism in Brazil. Social media has been instrumental in the launching of campaigns for better and cheaper public transportation\(^{59}\) and reducing electoral campaign waste,\(^{60}\) as well as for protests against the 2014 World Cup (which were fairly significant prior to the games but less impactful than expected during the actual event), and the Olympic games, to be hosted in 2016.\(^{61}\)

Although it is unclear whether it began online, in June 2013, the Free Fare Movement (Movimento Passe Livre) utilized social media for organization and mobilization of protestors. The movement, which originally demanded free bus fares for students and workers, also called for universal access to transportation and a shift in the transportation system from private to public management.\(^{62}\) WhatsApp, Facebook, Twitter, and Instagram were widely used to convene demonstrations by internet users and to disseminate information in real-time regarding associated protests in Brazil's main capitals. Uprisings received immediate coverage by anonymous users who uploaded videos, photographs, and information to social networks.\(^{63}\)


60 The “Quem Suja Agora” Facebook page was created to monitor and denounce the refusal to collect electoral campaign waste: https://www.facebook.com/quemsujaagora.


Violations of User Rights

Brazil made noteworthy progress in establishing a foundation for internet user rights with the passage of Marco Civil da Internet, a so-called constitution for the internet (Bill No. 2.126/11), which was signed into law in April 2014. The groundbreaking legislation establishes the rights to freedom of speech, communication, and 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. As the first overarching internet legislation of its kind, it is expected to serve as a model for other nations as they navigate this dynamic—and pervasive—new frontier.

The Brazilian Federal Constitution forbids anonymity but protects freedom of speech, including cultural and religious expression. Specific statutes and regulations also ensure freedom of the press. Cybercrime initiatives, cross-border cyberattacks, surveillance, and court rulings related to the internet made headlines in 2013 and 2014 for their impact on regulation of computer intrusion, brand infringement, discriminatory content, and governmental espionage. Brazil also continued to see instances of local officials bringing defamation suits against bloggers and online journalists. One blogger faced a prison sentence for a fictional story he posted online, although his sentence was converted to community service.

In recent years, various legislative initiatives have directly affected freedom of expression rights. The Azeredo Bill (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. Another initiative still under consideration in the Senate since 2008 (Bill 494/08) aims to impose a series of obligations on ISPs, websites, and blogs to ensure cooperation with the police in pedophilia investigations.

Several recent court cases concerning defamation may pose threats to freedom of expression online. In 2012, blogger Ricardo Antunes was sued and arrested in the state of Pernambuco, under accusations of charging BRL 2 million (approximately US$880,000) in order to refrain from publishing a corruption story about a businessman on his blog, Leitura Crítica (Critical Reading). He was granted a writ of habeas corpus and released in March 2013. While there has not yet been a judicial...
In another, 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 plans to appeal the ruling.

In October 2013, São Paulo appeals court judge Miguel Ferrari Júnior ordered the removal of information regarding slave labor accusations against Pinuscam, a wood supplier, posted online by media organization *Repórter Brasil*. The materials published by *Repórter Brasil* concerned a 2012 inspection in which the Department of Labor Justice rescued 15 workers who had been subject to slave-like conditions. The judge ordered the removal of the content posted online and banned the outlet from publishing anything further related to the case, as such posts could tarnish Pinuscam’s image. Given that the court order essentially prohibited investigative journalism, the judge later reconsidered its decision, allowing news about Pinuscam to be posted on *Repórter Brasil*’s website.

As previously mentioned, several legal provisions, including Article 57-D of the recently amended Electoral Act, 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 common. Despite the potential for such user registries to be employed to punish users for critical online speech, as of June 2014 there were no reports of such actions, nor were there reports of government efforts to track netizens participating in discussions critical of the government.

Further restrictions on anonymity have been urged by lawmakers in regard to public access points such as LAN houses, with the suggestion that internet communications be recorded in order to prevent cybercrimes. Such surveillance, lawmakers say, would also allow LAN houses to avoid liability for wrongful acts committed by users. Legislation of this kind already exists in São Paulo and Rio de Janeiro. A bill regarding “Centers of Digital Inclusion,” which includes mandatory
registration of LAN users, is currently under study by the Senate where it has been approved by several commissions and is now awaiting a final vote in plenary session. If finalized, the statute will regulate LAN houses as “multi-purpose entities of special interest for digital inclusion,” requiring them to register all users and to keep a directory of individual identification. The bill does not define how long such data must be kept, nor does it specify procedures for data requests.

While there is no evidence of extralegal surveillance online, government efforts to collect user data have increased significantly in recent years. With a total 1,085 data requests sent to Google between July and December 2013 and 44 such requests sent to Twitter, Brazil is ranked by both companies as third worldwide in number of requests for user data, following the United States and Japan. Brazil also claims third place (following Turkey and the United States) in Google’s ranking of countries issuing requests for content removal.

Threats, intimidation, and violence against online journalists and bloggers have continued in recent years. In late April 2012, Décio Sá, a longtime political journalist and blogger who wrote for the newspaper O Estado do Maranhão and ran a blog by the name of Blog do Décio, was shot to death while sitting in a bar. Police suspect that he was targeted for his reporting. Sá was killed two months after the murder of Mario Randolfo Marques Lopes, a combative blogger who ran a local news website in Barra do Piraí, a town about 90 miles northwest of Rio de Janeiro. Defendants in the Décio Sá case—currently pending—have yet to face trial by jury.

Both cases are emblematic of a common plight for provincial journalists in Brazil. Since they are not linked to major urban media outlets, these journalists 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.

In May 2013, federal policemen seized Ruy Sposati’s computer and sound recording equipment without a warrant while he was documenting the forced removal of an indigenous population in the state of Mato Grosso do Sul from land the government had decided to repurpose for development. Sposati, who worked as a journalist for the Indigenous Missionary Council (Conselho Indigenista
Missionário), has often spoken out against violence targeting journalists, specifically those covering sensitive topics.82

Brazilian journalists and photographers frequently faced intimidation during the June 2013 Free Fare Movement protests, especially by police officers. Social media proved crucial in reporting such abuse.83 Journalist Fernando Mellis, who was covering the street demonstrations for the Portal R7 website, was attacked by police officers with clubs in São Paulo. Reporter Leandro Machado, of Jornal Folha de São Paulo, and photographer Leandro Morais, of the news site UOL, were brought into custody for supposedly “disrupting police operations” during the protests, despite having identified themselves as journalists.84 Reporter Giuliana Valloni of Jornal Folha de Sao Paulo and photographer Sérgio Andrade da Silva of Futura Press were each shot in the eye with rubber bullets while reporting.85 Tear gas and stun grenades were also used to constrain protesters, reporters, and passersby in São Paulo, Rio de Janeiro, Belo Horizonte and Fortaleza.86 Many other attendees were taken into custody.

In August 2013, two unidentified gunmen shot at the house of journalist Ângelo Rigon, known in the state of Paraná for publishing accusations against local politicians on his personal blog. Despite five shots having hit the house, no one was injured. Ângelo constantly receives death threats, however.87 In February 2014, attorney Joel Caetano da Silva Filho Neto attacked Ribeiro Souza, a journalist at the radio station Paiaia FM, and his 15-year-old son in their home. Both were punched and kicked, and their lives were threatened. According to Souza, he had uncovered a malpractice scheme being led by Neto that targeted retirees in the city.88 In April 2014, reporter Bruno Amorim, who was working for O Globo newspaper in Rio de Janeiro, was beaten and arrested. Bruno was covering the eviction of residents from a private building in a slum in the northern part of the city and was accused by the police of disrupting their work and throwing rocks at policemen. No charges were made against him and he was released on the same day.89

In April 2013, a Brazilian cybercrime law commonly referred to as “Lei Carolina Dieckman” came into force. The law's adopted nickname comes from actress Carolina Dieckman due to the fact that the legislation took center stage after nude photos of her were distributed online in early 2012.90 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 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.

Cyberattacks have also been raising concerns in Brazil, with targets ranging from online banking websites to governmental agencies and energy plants. As of mid-2013, the country was listed among 10 nations most targeted by cyberattacks. Although there were 208 distributed denial-of-service (DDoS) attacks in the first quarter of 2013 (as compared to 200 during the same time period in 2012) the attacks targeted only 154 companies, meaning that many of those affected were hit more than once. Of these, 35 percent were large corporations, 32 percent were retail stores, 22 percent were media or entertainment outlets, 7 percent were IT companies, and 4 percent were governmental agencies. Cyberattacks affecting Brazil’s banking sector have been on the rise in recent years, and Brazil is now ranked among the top three target countries for such attacks, along with the United States and Japan. In the first three quarters of 2013, the country had the second largest malware detection system for online banking, second in scope only to the United States.

In early 2014, the hacker group Anonymous announced that official websites linked to the FIFA World Cup Games in Brazil would be targeted by future cyberattacks. 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. While the Anonymous attacks were preceded by public warnings, the threat of cyberattacks from other countries was not publicly foreseen.

While experts agree that in general, too little attention has been given to cybersecurity and related investments in telecommunication infrastructure in Brazil, Brazilian authorities seem to have accurately assessed the threat level surrounding the World Cup. A handful of companies, including Italian digital firm Tiger Security, were hired specifically to identify and fend off threats from domestic and international actors during the June to July 2014 games. 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.”

de Janeiro’s military police—appeared to be coming primarily from outside Brazil, namely from India, Turkey, Europe, Mexico, and the United States.98

Cambodia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>Limits on Content</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Violations of User Rights</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>47</td>
<td>47</td>
</tr>
</tbody>
</table>

Population: 14.4 million

Internet Penetration 2013: 6 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- A draft Cybercrime Law leaked in 2014 threatens to criminalize poorly-defined categories of online expression under a committee led by the prime minister (see Violations of User Rights).

- As social media fuelled support of the political opposition in advance of July 2013 elections, the National Election Committee warned internet users not to post “wrong information” online (see Limits on Content).

- Police used the threat of criminal defamation charges to compel two separate Facebook users to delete posts containing allegations about corrupt officers (see Violations of User Rights).

- Imprisoned land rights activist Yorm Bopha was released on bail in November 2013 after sustained civil society campaigns raised her profile online and overseas; her appeal is pending (see Limits on Content).
FREEDOM ON THE NET 2014

Introduction

The internet is partly free in Cambodia, and is therefore a rare source of uncensored information in comparison to other media, though it still reaches a limited portion of the population. The July 2013 National Assembly elections saw the widespread use of digital tools, especially amongst young voters, to exchange views, debate, and organize. Notably, the main opposition Cambodia National Rescue Party (CNRP) embraced social networks to campaign, which offset their virtual exclusion from state-controlled media coverage. News that CNRP leader Sam Rainsy would return from exile to campaign for the first time since 2009 was broken on social media,¹ and subsequently ignored by every television station in the country.²

Despite incremental gains by the CNRP and others, the incumbent Cambodian People’s Party (CPP) won by a narrow margin and Prime Minister Hun Sen retained power, according to the National Election Committee (NEC). Their count was heavily contested by the opposition as well as independent observers.³ Elected CNRP parliamentarians refused to take their seats in the National Assembly for the duration of this coverage period,⁴ and their supporters used on- and offline methods to call for Hun Sen's resignation and an independent investigation into voting irregularities.⁵ This activity prompted fears of increased censorship and unconfirmed reports that one internet service provider (ISP) temporarily blocked Facebook in August. “We have nothing to gain by closing Facebook, and we have no criminal law regarding the internet,” Information Minister Khieu Kanharith said, after access to the platform was restored.⁶

The government has been in the process of drafting an anticybercrime law, however, since 2012. Draft provisions leaked in April 2014 penalized poorly-defined categories of online expression.⁷ Even without such a law, internet freedom has begun to erode. At least three blogs hosted overseas are blocked on multiple ISPs for perceived antigovernment content. In 2013, police in two different cities threatened Facebook users with criminal defamation charges for posts alleging corruption in traffic enforcement. Death threats and negative rhetoric, particularly targeting those speaking out for Vietnamese migrants in Cambodian society were another troubling development of the past year. These cases of intimidation help encourage self-censorship online among bloggers and the wider population. The overall climate for political expression looked set to deteriorate further after demonstrations by CNRP supporters along with garment workers arguing for a higher minimum wage sparked

---

³ The Electoral Reform Alliance, “Joint Report.”
Cambodia

a violent crackdown resulting in the death of five people, dozens of injuries, 23 arrests, and an arbitrary ban on demonstrations in January 2014.  

Obstacles to Access

The International Telecommunication Union reported internet penetration in Cambodia, while increasing steadily, remained comparatively low at 6 percent in 2013. Cambodia’s Ministry of Posts and Telecommunications (MPTC) reported 3.8 million Internet users as of December 2013. Mobile phone penetration was at 134 percent due to the fact that many Cambodians own more than one low cost phone.

Historically, the absence of an extensive fixed landline network restricted internet penetration in rural Cambodia. Wireless broadband is helping to bridge a significant digital divide between rural and urban internet users, though a striking economic disparity persists. About 98 percent of internet users today have wireless access via satellite or Wi-Fi, according to the MPTC.

As in 2013, more than 20 ISPs were operating in the Cambodian market—government accounts cite as many as 27—offering competitive rates for high-speed internet, at around US$12 a month. In June 2013, the country’s largest ISP, EZECOM, announced that it plans to construct Cambodia’s first submarine fiber-optic internet cable. The cable will connect Cambodia with the rest of the world via the Asia-American Gateway. Scheduled for completion in October 2014, it is expected to greatly improve internet speeds and reduce costs for end users.

In the meantime, poor infrastructure still limits access. 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.

Language is another barrier, since few online applications are coded in Khmer. However, technology companies and information and communication technology (ICT) experts have made significant investments into the development of Khmer language applications. The Khmer Unicode font became widely available after the government recognized it as a standard in 2010. Both Google’s Khmer

---

12 O.U. Phannarith, Head of CamCERT and Permanent Member of Cybercrime Law, Working Group of National ICT Development Authority, “Cambodia Effort in Fighting Cybercrime in the Absence of Law,” slideshow presented at the Asia Pacific Regional Mock Court, Jakarta, Indonesia, September 18-19, 2012.
13 Heimkhemra, “Cheap Data, Better Tech Putting More Cambodians Online.”
Cambodia

translation tool and an English-Khmer translation system by local developers Sous Samak and Kim Sokpheap were launched in 2013. With these efforts, it is hoped that Khmer speaking netizens will be able to read non-Khmer content and vice versa, connecting Cambodian netizens to a broader audience and a wider pool of information.

With poor transportation and electricity coverage, mobile phones offer the most convenient access to a range of services including radio, music, and video, as well as web access. Mobile phone users surpassed the number using fixed landlines surprisingly early in Cambodia, and have gained popularity since 2000 even at the bottom of the economic pyramid, thanks to the free SIM cards, affordable handsets, and bonuses offered by service providers to attract consumers.

There are currently 7 such providers operating in 2014, down from 10 the previous year following several mergers and the addition of some newcomers. The market remains competitive despite two attempts by the MPTC to set the price of mobile calls in 2013, which observers said were designed to protect companies with links to officials from losing out to their competitors. The ministry banned mobile providers from offering bonuses in April, but withdrew the restriction after a public outcry. On November 28, 2013, the MPTC ordered all mobile network providers to comply with prices outlined in a 2009 government directive.

Mobile users and the business community again voiced objections, and the ban was revoked in December following a meeting of relevant stakeholders, including the MPTC and mobile network providers. It was the second time in seven months that the ministry was forced to cancel an order within 20 days of issuing it.

With the exception of one short-lived attempt by the NEC to ban SMS nationwide in advance of a 2007 election under a law prohibiting campaigning immediately before a vote, no government shutdowns of internet or mobile access have been documented in Cambodia.

In theory, the government welcomes and supports technology and infrastructure developments. However, despite public claims to support freedom of expression by Information Minister Khieu Kanharith and others, officials at both local and national levels have taken steps to curtail internet

Cambodia

access through ad hoc circulars and announcements. Challenges to these have yielded mixed results. A 2010 plan to strengthen internet security through a state-run exchange controlling all local ISPs was shelved due to popular opposition. A 2012 circular equated online gaming with terrorism, economic crime, and pornography, and ordered all internet cafes within a 500-meter radius of educational institutions in the capital, Phnom Penh, to close—an order which observers said would affect almost every venue in the city. Penalties for failing to comply with the circular include forced closure, the confiscation of equipment, and even arrest, though it has yet to be implemented. Most recently, in December 2013, on the other hand, authorities in northwestern Siem Reap province threatened access for the wider population when they announced the closure of more than 40 internet cafes for supposedly distracting youth with online games. Owners must gain official permission to reopen and, if denied, there is no known mechanism for appeal.

In September 2012, the Telecommunication Regulator of Cambodia was established by royal decree and charged with formulating fair and transparent policies, strengthening market competition, and encouraging the further development of Cambodia’s ICT market outside the direct control of the government. It has yet to act publicly on its remit and whether it will be able to operate independently and effectively is not known.

Limits on Content

Commentators noted an increase in online political discourse around the 2013 election—especially on social networks like Facebook and media-sharing platforms such as YouTube—and heralded the continued development of digital democracy in Cambodia. The sites continued to play a significant role after the polls as users spread videos and information alleging voting fraud, though these have yet to result in an investigation. While only a handful of political blogs hosted overseas are blocked in Cambodia, several officials made statements warning internet users not to misuse social networks in the past year, prompting fears that censorship could yet be extended online. Online activism saw more success on social and human rights issues, helping to achieve the release of a jailed land rights activist on bail.

Websites showing pornography or sexually explicit images are subject to blocking in Cambodia on moral grounds. Politically motivated blocking has not yet been systematically applied, although it has been observed on a case by case basis. Implementation in either case is nontransparent, apparently based on informal communications between government officials and service providers, which

24 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.
provide no avenue for appeal. In early 2011, for example, Minister of Posts and Telecommunication So Khun asked mobile phone operators to “cooperate” in blocking websites “that affect Khmer morality and tradition and the government,” according to The Phnom Penh Post, citing internal MPTC minutes.30

As a result, censorship is hard to verify. In 2009, the Cambodian Center for Human Rights (CCHR) reported the AngkorNet ISP was blocking access to a report by the UK-based NGO Global Witness, because it criticized government corruption. AngkorNet confirmed the content was temporarily inaccessible to subscribers, but said it was due to a technical error.31 Since then, international NGO and news websites have been widely available.

In 2011, several ISPs briefly blocked the international hosting service Blogspot after the popular overseas-run Cambodian blog KI-Media ran a post calling the prime minister and other high-level officials “traitors.”32 While Blogspot was restored, a handful of individual sites hosted on the service, including KI-Media, critical citizen journalist blog Khmerization, and a blog by the Khmer political cartoonist Sacrava, were blocked again the following month. The government denied involvement, but one ISP posted error messages saying the sites were blocked on MPTC orders, and The Phnom Penh Post leaked the contents of an email sent by an MPTC official thanking 10 ISPs for implementing the blocks.33 At least three of the sites remained inaccessible on some ISPs without the use of circumvention tools in 2014.

Partly as a result of events like these, self-censorship remains an issue amongst many Cambodian bloggers (or “cloggers”), who often fear the repercussions of sharing political views online.34 Events like Barcamp, a networking gathering for technology professionals, attest to the increasing number of bloggers, especially well-educated people in their twenties.35 But the majority blog about personal, rather than political events.36 Nevertheless, there are a number of political websites available to Cambodian youth, and many continue to read even blocked content using privacy tools such as virtual private networks (VPNs), which disguise online activity via an uncensored connection overseas. The government has not tried to curb access to these tools, although there is no data indicating how widely they are used.

In the run up to the July 2013 national election, there was a marked increase in the use of SMS and the internet by political parties and young Cambodians alike, to discuss, debate, and share information and opinions about the upcoming polling. With technical support from the Cambodian NGO

Cambodia

Open Institute and the International Foundation for Electoral Systems, the NEC launched a voice-based information service for voters.37 Perhaps most significantly, the opposition used Facebook to communicate with supporters and to coordinate rallies, despite remaining marginalized in public discourse due to strict media controls.38 Some of these controls affected websites run by media outlets, though possibly through internal pressure rather than technological censorship. One reporter said his Khmer-language newspaper article about a May 2013 opposition rally was “mysteriously removed” after he uploaded it.39 Overall, however, many observers credited the CNRP’s 55 seats to their online popularity; the CPP lost some seats but retains a majority with 68.40

While politicians abused their opponents online,41 there was no noticeable deployment of paid commentators distorting discussions according to a political agenda during this period. Still, many fear the CPP could yet restrain political expression online. In May 2013, the NEC told social media users not to “create fear, confusion or a loss of confidence in the secrecy of the vote.”42 On the same day, in remarks made to students, Information Minister Khieu Kanharith warned them not to use Facebook to impugn the reputation of others.43 On August 7, many Facebook users reported the site was unavailable for several hours on the popular Metfone ISP, prompting fears the government had blocked it to suppress online activism.44 Khieu Kanharith denied responsibility for the disruption, which Metfone attributed to technical error.45

In the aftermath of the election, opposition supporters continued to use social media to spread evidence of alleged voting fraud and call for an independent investigation, but these efforts have yet to see results. When antigovernment protests swelled in the capital in December and were violently suppressed in January 2014, online networks helped challenge the censored state media account of events,46 even as a ban on public gatherings attempted to prevent such information from mobilizing effective political challenges.

A range of netizens and grassroots activists have used new media and other online tools to make an impact on less overtly political issues. Online activism like this has raised awareness of compelling issues in the public interest, such as the environment and traffic safety, and contributed to Cambodia’s social and political development. In one recent success, land rights activist Yorm Bopha was released on bail in November 2013 after a year and a half behind bars in relation to allegations that she was

45 Seangly and Worrell, “Facebook Safe: Government.”
involved in the assault of two motorbike taxi drivers, which her supporters characterized as politically motivated. The Supreme Court ordered her case to be reinvestigated and reheard by the Phnom Penh Court of Appeal following sustained local and international campaigns for her release, including online petitions and general awareness-raising via social media and NGO websites.

**Violations of User Rights**

In April 2014, digital freedom activists expressed concern over a leaked cybercrime law which was drafted without public consultation. While it is not known if the draft will be passed in its current form, it criminalizes a range of ill-defined activities such as generating “instability,” would punish online slander worse than the same crime committed offline, and allows prosecutors rather than judges to order the retention of computer data in criminal investigations. Implementation of the law would be at the discretion of a government committee headed by the prime minister. During the coverage period, police questioned Facebook users who had posted allegations of misconduct related to enforcement of motorcycle registration rules, though the criminal defamation charges the individuals were threatened with never materialized. Accounts of death threats circulating online also rose. The climate of intimidation was reinforced by a harsh security response to offline demonstrators, which resulted in several deaths.

Freedom of expression and freedom of the press are upheld under Article 41 of the Cambodian Constitution. The constitution also upholds the provisions in the International Covenant on Civil and Political Rights, ratified by Cambodia in 1992, and the Universal Declaration of Human Rights, both of which guarantee the right to freedom of expression and information.

Despite these protections on paper, freedom of expression is not upheld in practice. Provisions in the 2010 penal code governing criminal defamation and incitement have been used to punish journalists who criticize the government. The authorities regularly punish dissent through threats, judicial harassment, and sometimes violence. In 2012, Human Rights Watch reported “at least 35 political and social activists and residents involved in defending human rights, opposing land grab, and demanding better working conditions were killed, wounded, arbitrarily arrested, threatened with arrest, or kept in exile by Cambodian People Party (CPP)-led security forces and the CPP-controlled judiciary.” These punishments are a powerful disincentive to individuals and organizations that wish to express their own views.

The election and the contested result served as a catalyst for intensified restrictions on political association. In early January 2014, opposition supporters protesting against the election result joined garment workers campaigning for a higher wage in the capital. Security forces responded violently

---


and banned demonstrations until “public order and security are restored.”

A number of land activists, CNRP political activists, and media freedom advocates were subsequently detained or dispersed. Draft laws to regulate nongovernmental organizations and unions pending since 2010 and 2011 respectively contain repressive provisions that threaten to further chill freedom of association, and could have a negative impact on online expression in future political movements. The draft law on unions, for example, contains provisions that would make trade unions vulnerable to dissolution, and provides too much discretion for the government to regulate the process. The laws are expected to be reintroduced in 2014.

A cybercrime law currently being drafted by the government could add another tool to the legislative arsenal used by officials to repress their critics. While the legislation will ostensibly combat cybercrime, the use of existing laws to limit free expression along with the ad hoc, opaque efforts to regulate internet access and content set troubling precedents for the law’s potential abuse by the state.

A lack of transparency and consultation over the law’s development since it was proposed in May 2012 is further cause for concern. A ministerial press unit initially characterized it as a law to “prevent ill-willed groups from spreading false information” that could “affect national security,” citing 2012 SMS rumors of a violent political clash in Phnom Penh as an example. Officials later said it would be modeled on European Union legislation to “protect formal, private and copy-righted data from hacking, or the destruction of users’ formal data, especially banks and related institutions.” Civil society organizations have been denied a chance to formally review or provide input for a draft.

In April 2014, the freedom of expression advocacy group Article19 obtained a copy of the Cybercrime Law Draft V.1 and published an unofficial translation. Some of its worrying provisions include Article 28(3), which prohibits publications “deemed to generate insecurity, instability and political cohesiveness [sic],” Article 28(4), which prohibits “undermining the integrity of any governmental agencies;” and Article 28(5), which prohibits publications “deemed damaging to the moral and cultural values of the society,” including those which are considered “manipulation, defamation and slanders [sic].” The draft carries potential prison sentences of one to three years and fines ranging from KHR...
Cambodia

2 to 6 million ($490 to $1,480). By contrast, offline slander is punishable by a maximum of one year behind bars. The lack of adequate definitions in the law is especially concerning considering the proposed make-up of a National Anti-Cybercrime Committee to enforce, investigate, and regulate cybercrime laws, established in Article 6, which will consist of high-ranking members of government under the chairmanship of the prime minister. The draft further grants prosecutors authority to issue court orders to preserve computer and traffic data for purposes of criminal investigation, rather than judges. The timeframe for revisions of the draft and passage of the law is not known.

Some authorities have already extended existing defamation and incitement laws to online content. In 2010, the Phnom Penh Municipal Court used Article 495 of the new penal code to sentence UN Food Program employee Seng Kunnaka to six months’ imprisonment and a fine of KHR 1 million ($250) on a charge of incitement to commit a felony after he printed articles from KI-Media for a handful of colleagues. In 2013, police twice threatened Facebook users who had posted allegations of misconduct related to the enforcement of motorcycle registration rules. Teacher Phel Phearun was questioned and threatened with a defamation charge in May after his account of an encounter with Phnom Penh traffic police, posted on Facebook in January, sparked an online debate about police corruption. Six months later, in the northwestern city of Stueng Treng, police detained 23-year-old marketing manager Cheth Sovichea for a day after he used his Facebook profile to accuse local officers of confiscating unregistered motorcycles to solicit bribes. He avoided a defamation charge by removing the offending post and publicly apologizing.

Phnom Pehn-based freelance journalist Rupert Winchester faced a defamation suit during the coverage period for an article about a businessman published on his personal blog in June 2013. In July 2014, outside the coverage period of this report, he was fined KHR 8 million ($2,000) and ordered to pay KHR 1 hundred million ($25,000) in damages, in a verdict local and international press groups called detrimental to online freedom of expression.

The internet has itself become a medium for threats and intimidation of public figures in Cambodia. In December 2013, members of the CNRP said their deputy leader Kem Sokha had received a death threat containing photographs of a gun and ammunition via Facebook, apparently from an account belonging to a police officer, who denied sending it. Also in December, the leader of NGO the Cambodian Center for Human Rights Ou Virak was targeted with a barrage of online abuse via Facebook and email after he criticized the leader of the CNRP for using discriminatory language about

---


Cambodia

Vietnamese immigrants. Though negative rhetoric spiked, however, and physical harassment of traditional journalists continued unabated, there were no accounts of violence in retribution for online activity during the coverage period of this report.

Government surveillance of citizens’ digital activity is not known to be technologically advanced or widespread in Cambodia. However, in February 2012, a joint Ministry of Interior and MPTC circular ordered internet cafes to set up surveillance cameras and store footage for three months; phone shops and telecommunications operators were told to register subscribers’ national ID cards or international passport and visas on the grounds that such measures would “better promote protection of national security, safety and social order.” The operators “are obliged to provide necessary documents including users’ identity cards and used data”—which must be stored for six days—to designated officials “for purposes of investigation of any offense which is involved in issues of national security, safety and social order.” Under the internal circular—which only came to public notice in August 2012—providers must also notify existing subscribers of the new requirements and are entitled to temporarily suspend service if they fail to produce ID within a month. As of April 2014, in accordance with Cambodia’s habitually slow pace of adopting new regulation, the requirements had yet to be implemented, though civil society groups fear the impact of such supervision for public debate and social activism. The circular’s vague definition of what constitutes an offense, the lack of judicial oversight over officials’ requests for user data, and the threat of unspecified fines or licensing restrictions for telecommunications operators who fail to comply, all represent a lack of respect for digital rights.

While experts say technical attacks frequently go unreported in Cambodia, civil society groups and government critics have not been systematically targeted by criminal hackers. Government websites are vulnerable to technical violence, which increased during the 2013 election period. In July 2013, the NEC website was temporarily disrupted following allegations that the government was trying to register illegal immigrants to vote. In September, the global hacking group Anonymous posted an online declaration of war against the Cambodian government following the fatal shooting of a bystander, Mao Sok Chan, at a clash between military police and opposition protesters. Several websites belonging to ministries, the police, educational institutions, and other organizations with ties to the government were briefly disabled in attacks attributed to the group. However, four alleged members of the hacking group Anonymous Cambodia were reportedly arrested during the cover-
age period of this report. Although the timing could be a coincidence, the arrests could help the government build a case for the public in favor of a restrictive cybercrime law that fails to distinguish adequately between illegal acts and legitimate expression.

Canada

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>N/A</td>
<td>Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>n/a</td>
<td>3</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>n/a</td>
<td>3</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>n/a</td>
<td>9</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>N/A</td>
<td>15</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 35.3 million
Internet Penetration 2013: 86 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Free

Key Developments: May 2013 – May 2014

- In October 2013, parliament introduced Bill C-13, which was intended to remedy concerns over cyberbullying but which also contains troubling provisions regarding warrantless disclosure of user data (see Violations of User Rights).
- Bill S-4, also known as the Digital Privacy Act, was introduced by parliament in April 2014 and includes requirements for organizations to disclose security breaches that put Canadians at risk. However, this bill could also reduce court oversight in cases related to copyright infringement (see Violations of User Rights).
- A Federal Court of Appeals ruling on January 31, 2014 found that section 13 of the Canadian Human Rights Act (CHRA), the legislation that provides for hate speech penalties, does not violate the constitutional right to freedom of expression. However, prior to this decision, parliament voted to repeal section 13 in June 2013; the repeal officially took effect in June 2014. Currently, hate speech can still be regulated under section 320.1 of the criminal code (see Violations of User Rights).
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, in addition to a well-developed set of rules regulating intermediary liability in cases of copyright infringement. Canada’s communications regulator has avoided regulating “new media” entities, which encompasses a broad range of internet-based companies offering video and other content services. Further, Canada’s privacy commissioner has aggressively focused on internet-related concerns, particularly those involving search functions and social media.

Despite these strengths, there remains considerable unease among many Canadians with respect to online rights. Proposed legislative reforms, including the Digital Privacy Act (Bill S-4) and the Protecting Canadians from Online Crime Act (Bill C-13, also known as the “cyberbullying” bill), have generated concern among many Canadians with regard to potentially negative provisions included within the bills, such as plans to expand the scope of voluntary disclosures of personal information without court oversight. Additionally, Canada’s role in global surveillance activities was revealed over the past year through the NSA documents leaked by Edward Snowden, causing many to question the sufficiency of surveillance oversight in Canada.

The vertically integrated telecommunications market, in which a handful of companies dominate broadcast, telecom, wireless, and internet access, has also raised considerable fears about the state of competition within Canada and the potential for those companies to use their privileged position to violate net neutrality, increase access costs, or engage in uncompetitive behavior. The Canadian Radio-television and Telecommunications Commission has developed vertical-integration policies, but their effectiveness is open to question.

Obstacles to Access

According to the International Telecommunication Union (ITU), Canada had an internet penetration rate of nearly 86 percent in 2013, compared to 83 percent in 2012 and 77 percent in 2008. 1 Similarly, Statistics Canada reported in 2013 that 83 percent of Canadians use the internet. 2 DSL broadband internet access service is available in all provinces and territories. By the end of 2010, 85 percent of households were located within the DSL broadband footprint, and 15 percent of households were served by either fiber-to-the-node or fiber-to-the-home connections. 3

Broadband internet access through cable modems is available in all provinces and territories except the northernmost territory of Nunavut, and by the end of 2013, approximately 33 percent of the

---

population had fixed broadband subscriptions.\(^4\) Although satellite broadband internet access service is available throughout Canada, it is generally used to provide broadband internet service in the more rural and remote areas of the country. Wireless internet access is the fastest growing sector for internet service in Canada: over 48 percent of Canadians used wireless internet services in 2012, compared to about 26 percent in 2010.\(^5\)

According to the ITU, Canada had a mobile phone penetration rate of over 78 percent in 2013.\(^6\) Mobile carriers have deployed a number of newer technologies to provide mobile broadband service, including HSPA+ and LTE.

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 has an internet penetration rate closer to 63 percent.\(^7\) 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.

There is a wide range of content available in both of Canada’s official languages (English and French) as well as many other languages. 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.

There are no government restrictions on bandwidth, although access providers frequently offer services with caps on bandwidth that result in increased fees. 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 could facilitate greater control of content and the use of surveillance technologies.

To operate as a Canadian telecommunications carrier, a company must meet the requirements in section 16 of the Telecommunications Act. In 2012, Canadian telecommunications revenues amounted to $43.9 billion. Ten companies and their affiliates accounted for 93 percent of this total revenue, with the remaining smaller companies earning combined revenues of less than $2.9 billion. Each company’s revenue falls within the 10 percent maximum of total Canadian telecommunications revenues, as required by subsection 16(6) of the Telecommunications Act.\(^8\)

Canadians have a choice of wireless internet providers, virtually of which are privately owned (the notable exception being SaskTel, a government-owned provider in the Province of Saskatchewan).

---


\(^8\) Statistics Canada, Table 358-0152.
Canada

There are at least three providers 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, the market is dominated by three companies: 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 emphasized the need for more competition in this market.

The Canadian Radio-television and Telecommunications Commission (CRTC), the regulatory body that oversees the communications industry, operates largely independently from the government. In 1976, the federal government created the CRTC by consolidating multiple federal regulatory bodies that had jurisdiction over electronic communication media. The CRTC's authority is derived from two federal acts: the Broadcasting Act and the Telecommunications Act. Section 7 of the Telecommunications Act outlines the broad policy objectives pursued by the Act and, by extension, the CRTC, in the field of telecommunications. Section 7 enumerates nine specific objectives that feature two key themes: consumer telecom services and a strong domestic telecom industry. Regulation is intended to be limited and focused on instances where the market is patently unable to achieve the intentions and goals of the Act.

The chair and commissioners of the CRTC are appointed by the government, and 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 2011.9

Limits on Content

The Canadian government does not generally block websites or filter online content. Illegal content may be removed by private legal action taken through the court system.10 YouTube, Facebook, Twitter, and international blog-hosting services are freely available.

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).11 Accessing child pornography is illegal in Cana-

dashboard/


da under section 163.1(4.1) of the criminal code. 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, which will assess the site and, if necessary, obtain an independent, binding judgment from the National Child Exploitation Coordination Centre. An appeals process has also been put into place for cases in which content providers believe that their content has been wrongly blocked (though the list of blocked sites is not public since it would essentially provide a directory of child pornography). The project blocks approximately 1,000 child pornography images each year.

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. 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. 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.

Defamation claims may also result in the removal of content, as providers fear potential liability as a publisher of the defamatory content. Unlike legal protections against liability for copyright infringement by its users, providers may face liability for alleged defamation once alerted to the publication. A court may also order the removal of the content.

With the exception of the topics discussed above (child pornography, hate speech, copyright) there does not appear to be widespread self-censorship in Canadian online publications. 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.

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. The Canadian Radio-Television and Telecommunications Commission (CRTC) oversees the regulation and provision of internet services, and section 36 of the Telecommunications Act states that “a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public,” unless otherwise approved by the CRTC. Complaints can be filed with the CRTC for alleged violations. The provision is relevant in the net neutrality context since the CRTC has ruled that section 36 could be raised to counter an ISP controlling the content that it carries. The provision forms part of the net neutrality safeguards in Canada, which are called Internet Traffic Management Practices, or ITMPs. The CRTC has used the ITMPs to stop ISPs from blocking or throttling content.

---

12 *Criminal Code*, RSC 1985 c C-46 s 163.1(4.1).
13 *OpenNet Initiative*.
Canada

from throttling internet traffic, and the policies are currently being considered in the context of mobile video services.

Social media and communication applications have been widely used in Canada for the mobilization of political and social movements. For example, a social media campaign in 2012 successfully stalled a government proposal that would have allowed for increased monitoring and tracking of Canadians’ activities online. On February 13, 2012, then-Public Safety Minister Vic Toews infamously told the House of Commons that critics of his forthcoming lawful access bill could either stand with the government or “with the child pornographers.” Bill C-30 was introduced the following day, but within two weeks, a massive public outcry—much of it online—forced the government to quietly suspend the bill. A year later, the government openly acknowledged that the bill had been dropped.

The Twitter-based #tellviceverything campaign, invoking the idea that the government already has too much access to one’s private communications data, provided a perfect illustration of how the internet can fuel awareness and action at remarkable speed. Through thousands of tweets, Canadians used humor to send a strong message against Bill C-30. Alongside the Twitter activity were dedicated websites, hundreds of blog postings from commentators on the left and right of the political spectrum, thousands of calls and letters to MPs, and nearly 100,000 signatures on the Stop Spying petition hosted by the organization Open Media.

There are undoubtedly many factors that led to the successful fight against the bill. Toews’ comments placed the government on the defensive from the outset, and the substance of the bill generated criticism from both sides of the political spectrum. Yet the bigger story was the emergence of the public voice on digital policy. Justice Minister Rob Nicholson’s comments in announcing the defeat of Bill C-30 highlighted the impact of the public outcry:

“We will not be proceeding with Bill C-30 and any attempts that we will continue to have to modernize the Criminal Code will not contain the measures contained in C-30, including the warrantless mandatory disclosure of basic subscriber information or the requirement for telecommunications service providers to build intercept capability within their systems. We’ve listened to the concerns of Canadians who have been very clear on this and responding to that.”

The emphasis on responding to public concern highlights the public campaign’s effectiveness and the recognition of the need to incorporate broader perspectives into legislative and policy developments.

---


Violations of User Rights

Despite having a generally positive record for freedom of expression, Canada has, in recent years, taken some regressive steps, 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 requests. The country’s 30-year-old Access to Information Act (ATIA) is also highlighted as an obstacle given the long delays and regular use of exceptions to redact large amounts of information from released documents.

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. Section 1 of the Charter allows the government to pass laws that limit free expression so long as the limits are reasonable and can be justified. These laws and protections apply to all forms of speech, whether online or offline.

Two 2010 court cases—Globe and Mail v. Canada19 and R. v. National Post20—have dealt with journalistic privilege directly. While Canada’s Supreme Court Justices have stopped short of offering blanket confidentiality, they have stressed that compelling journalists to reveal sources should be extraordinary and not the rule, recognizing that investigative reporting plays an important role in society. Instead, tests should be applied on a case by case basis. In addition, the court ruled that journalists have the right to publish confidential material from a source, even when the source has no right to divulge the information or has obtained it by illegal means.

Copyright legislation in Canada includes specific protections for non-commercial, user-generated content (UGC). The drafting of this legislation was particularly focused on online mashups and other forms of remix expression. The non-commercial UGC provision, which took effect in 2012, legalizes both the creation and distribution of user-generated content provided that the work meets four criteria, including that it is non-commercial, there is attribution where reasonable, the original work was not infringing copyright, and the new work does not have a substantial adverse effect on the original.

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.21 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,

---

21 Criminal Code, RSC 1985 c C-46 s 320.1; OpenNet Initiative.
Canada

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.22

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.

Judicial rulings related to freedom of expression and defamation online have varied. In 2011, an Ontario Supreme Court decision in the case of Baglow v. Smith established that the threshold for prosecuting defamatory content from political blogs should be higher than in traditional forms of media, since the blogosphere is “a place where readers expect to encounter disrespectful comments and visceral rejoinders.”23 This case was originally decided by a summary judgment, or expedited ruling, in September 2011, as the judge deemed it to be a relatively straightforward case; however, the summary judgment was overturned by appeal in June 2012, and the full trial began on March 24, 2014. As of May 2014, the trial was still ongoing.

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.

Citizens can be subject to legal sanction depending on the material that is being accessed. They can be found guilty of possessing, accessing or even distributing child pornography if they post images of it on the internet.24 This also extends to text messages, such as in a January 2014 case of a teenager who had sent texts containing explicit images of another teenager and was convicted

---


of possession of child porn.\(^{25}\) Generally, writers, commentators, or bloggers are not subject to legal sanction because of what they post on the internet.

Website owners, bloggers, and internet users in general are not required to register with the government. However, identification is required in order to purchase a mobile phone through a telecommunications company. Pay-as-you-go phones can be purchased without ID, since no contract is required.

In a decision related to privacy protections for user’s identifying information, the Divisional Court in 2010 overturned an order in the case Warman v. Fournier requiring the named defendants, who run an internet message board, to produce documents identifying several users who posted allegedly defamatory comments on the message board. The Divisional Court found that the case engaged both freedom of expression and privacy interests under the Charter, and that these interests should be balanced against the public interest. It held that courts should adopt a process that provides for a balancing of the interests at stake before identity information is disclosed by a party, noting that otherwise, a plaintiff with no legitimate claim could, for example, misuse the court rules by bringing a frivolous action against an ISP for the sole purpose of identifying an anonymous internet commentator.\(^{26}\)

In the past year, the Canadian parliament proposed two pieces of legislation—Bill C-13 and Bill S-4—with implications for privacy and freedom of expression. Bill C-13, known as the Cyberbullying Bill, would make it illegal to circulate explicit images online without the subject’s consent, but would also grant legal immunity to telecommunication service providers who voluntarily hand over user’s information to the authorities.\(^{27}\) Bill S-4, the Digital Privacy Act, contained certain provisions that could enhance users’ privacy online, including making it mandatory to notify consumers when a company experiences a data protection breach. However, the bill could remove the court order requirements in cases of copyright infringement lawsuits, effectively moving to a notice-and-takedown system.

Both pieces of legislation contain positive attempts to protect individual’s privacy online; however, negative or vaguely worded provisions in the legislation require further consideration regarding their implications for individual’s rights online. By May 2014, the end of this report’s coverage period, both bills were still pending in parliament.

Users are allowed to use encryption software to protect their communications. Canadians are free to develop, import, and use whatever cryptography products they wish.\(^{28}\) There are no laws in Canada that restrict the use of encryption or other security tools,\(^{29}\) although Ottawa offices have told telecommunication companies that one of the conditions of obtaining a license to use wireless spectrum is to provide the government with the capability to bug the devices that use the spectrum. In


\(^{26}\) Warman v Fournier, 2010 ONSC 2126, 100 OR (3d) 648.


addition, as part of the requirements Ottawa has demanded companies to scramble encryption so that it can be accessed by Canada’s law enforcement agencies.30

The June 2013 revelations about the online surveillance practices of the U.S. National Security Agency (NSA) had a significant impact on discussions surrounding the practices and policies of the Canadian government as well, particularly as Canada is a member of the Five Eyes alliance (along with the United States, the United Kingdom, Australia, and New Zealand). It is difficult to know precisely what occurs with respect to online monitoring. The Communications Security Establishment of Canada (CSEC) maintains that it does not monitor Canadians; however, leaked documents revealing that U.S. and British intelligence agencies may have been able access to their citizens' data through the Five Eyes alliance calls this statement into question.

In Canada, Part VI of the criminal code governs the powers of law enforcement to engage in electronic surveillance of private communications when conducting criminal investigations. The criminal code requires the production of annual reports on the details of the interceptions that occur, though the information is aggregated and provides only limited insight into actual interception practices.

Canadian electronic surveillance for foreign intelligence is primarily undertaken by the National Defense's secretive Communications Security Establishment (CSEC), which operates in close cooperation with its U.S. counterpart and other allied intelligence networks. A commissioner is appointed to review the actions of the CSEC and produce annual reports commenting on the adherence of the agency to its legislative mandate in the National Defense Act of 1985. The commissioner’s annual reports, while providing some oversight, offer little additional transparency, as no statistics on the number of communications interceptions are reported.

Canada’s private sector privacy law (PIPEDA) requires consent for the collection, use, and disclosure of personal information along with appropriate disclosure of privacy practices. The law features a complaints mechanism that allows for individuals to direct complaints to the Privacy Commissioner of Canada, who is independent of the government. While this process provides some measure of oversight with respect to the collection, use, and disclosure of personal information by the private sector, the activities of law enforcement are less well known. The Supreme Court of Canada has ruled on the need for a court order or warrant for the disclosure of personal information by ISPs.

While oversight and review mechanisms exist regarding government surveillance, there are concerns about the sufficiency of the system. For example, past statements by the head of the CSEC indicate that the intelligence agency does not consider metadata to be subject to the same privacy protections accorded to content.31 Canadian privacy commissioners have also highlighted the privacy implications of metadata and information that is not typically classified as “content.” In May 2013, the Privacy Commissioner of Canada released a report on the privacy value of IP addresses, noting that one data point could lead to information on website habits that include sites on sexual preferences.32


In July 2013, Ontario Privacy Commissioner Ann Cavoukian issued a primer on metadata for consumers, asserting that such data may be more revealing than content.\(^\text{33}\)

In a decision on the case R. v. Vu in November 2013, the Supreme Court ruled that authorities must obtain specific authorization to search computers or other electronic devices located on the premises outlined in a search warrant, noting that the “privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets.”\(^\text{34}\)

There were no documented cases of violence or physical harassment of internet users in Canada for their online activities during the reported period.

There have been several high profile cyberattacks and data breaches in Canada, including some that have involved the government. In 2011, a cyberattack apparently launched from China targeted several government agencies, including Defence Research and Development Canada, the civilian branch of the Department of National Defence.\(^\text{35}\) Canadian universities have also reported a rise in cyberattacks over the past year.\(^\text{36}\) In May 2013, a study released by the U.K.-based International Cyber Security Protection Alliance stated that nearly 70 percent of Canadian businesses had experienced cyberattacks.\(^\text{37}\)


China

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>29</td>
<td>29</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>38</td>
<td>39</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>86</td>
<td>87</td>
</tr>
</tbody>
</table>

Population: 1.36 billion
Internet Penetration 2013: 46 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

* 0=most free, 100=least free

Key Developments: May 2013 – May 2014

- President and CCP General Secretary Xi Jinping framed the internet as a battlefield for ideological control and appointed himself the head of a top-level internet security committee (see Introduction).

- The State Internet Information Office consolidated content restrictions with a harsh crackdown on rumors under newly appointed “Internet Tsar” Lu Wei (see Limits on Content and Violations of User Rights).

- A September 2013 judicial interpretation criminalized a range of online content viewed more than 5,000 times or shared by 500 internet users (see Violations of User Rights).

- High-profile businessmen were among hundreds detained or interrogated for supposedly abusing their online influence as controls on microblogs tightened (see Violations of User Rights).

- Legal activist Xu Zhiyong was jailed for four years for disturbing order and “public spaces on the internet” in April 2014 (see Violations of User Rights).

- Telecommunications were shut off in a restive area of Xinjiang; and Uighur academic Ilham Tohti was charged with antistate activity via his website (see Obstacles to Access and Violations of User Rights).

- A court in Hainan jailed an internet police officer for accepting bribes to issue takedown notices via instant message to web platforms in his jurisdiction (see Limits on Content).
Introduction

On September 21, 2014, the Sina corporation’s Weibo microblog blocked mainland Chinese users from searching for the terms “boycott classes” and “Hong Kong.”1 The following day, students in the territory launched a week-long strike and occupied city intersections to protest against a Chinese government decision to screen candidates for chief executive in 2017 elections. Democracy activists swelled their numbers, and by early October, tens of thousands of people had taken to the streets.

Observers feared the Chinese Communist Party (CCP) would extend internet restrictions implemented on the mainland to Hong Kong in order to suppress the demonstrations. Rumors that police would shut down telecommunications networks spread on September 28. Protesters responded by downloading applications like FireChat, a tool from a San Francisco-based developer which establishes a mesh network between smartphones, allowing them to communicate within a given range without a cellular or internet signal.

In fact, this act alone illustrates the access, information, and digital rights enjoyed by Hong Kong residents under the “one party, two systems” framework in place since the city reverted from British to Chinese rule in 1997.2 The download page for FireChat is blocked in China, along with dozens of apps that could facilitate political assembly.

Hong Kong’s internet shutdown never took place.3 Mainland authorities shut off access via state-owned enterprises which dominate the mainland telecommunications market. But service providers in Hong Kong operate in a competitive environment that sustains an international financial sector, as well as the political and corporate groups who support Beijing. Internet in Hong Kong is faster than anywhere in the world except Japan and South Korea,4 and the chief executive must issue a warrant under a state of emergency to disconnect it.5

Hong Kong protesters launched Facebook pages to facilitate communication with both police and supporters overseas,6 and shared visuals of the umbrellas protestors used to shield themselves from tear gas and pepper spray.7 In mainland China, Facebook is blocked and censors shut off access to its photo-sharing platform Instagram on September 19 to stop the iconic images from spreading. In Hong Kong, the South China Morning Post documented unfolding events in real time on its website.8

---

2 Freedom on the Net 2014 does not provide a ranking and analysis of internet freedom in Hong Kong. Noteworthy incidents from the coverage period may be cited in the China report but are not considered in China’s score assessment.
In mainland China, the outlet was added to the list of international media websites that are blocked or filtered on October 5.\(^9\)

Hong Kong’s robust internet freedom was eroded during the demonstrations. Sina cancelled the Weibo accounts of some Hong Kong protesters, as did Tencent for its messaging service Weixin.\(^10\) Supporters of Occupy Central who downloaded an app supposedly connected with the movement found it had installed malware on their devices. Security experts pointed out that even FireChat and similar resources could potentially expose a user’s identity or location. Police detained several people, including a 13 year old, for allegedly conducting cyberattacks on government websites.\(^11\)

But the impact was much more significant in China, which Freedom on the Net ranked third worst in the world for internet freedom during the coverage period of this report, May 2013 through May 2014. Observers said censorship was more intense in October 2014 than it had been in June, during the 25th anniversary of the military crackdown on 1989 protests in Beijing. An estimated twenty activists were detained for expressing support for the movement online.\(^12\) Information authorities distorted popular discourse online by amplifying state media commentary and nationalist voices. These portrayed the rally as anything but a popular prodemocracy movement, including a foreign plot, and in at least one case, a demonstration of support for Beijing.

Similar tactics were used throughout the past year as China’s internet freedom deteriorated. In May 2013, the State Internet Information Office (SIIO) launched an unusually broad crackdown on rumors under newly-appointed CCP hardliner Lu Wei.\(^13\) In an internal speech at the National Propaganda and Ideology Work Conference on August 19, first publicized by military and party commentators, and later revealed in full by China Digital Times,\(^14\) President and CCP General Secretary Xi Jinping described online information control using stronger rhetoric than Hu Jintao’s “guidance” and “channeling.” “The Internet has become the main battlefield for public opinion struggle,” he said in the speech, which provided the ideological underpinning for the internet freedom decline.\(^15\) A month later, Lu Wei 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.\(^16\)

The emphasis on continuity disguised an important shift. The party’s Central Propaganda Department is traditionally considered the bastion of censorship, but the SIIO, established in 2011, is an

\(^9\) See, https://twitter.com/george_chen/status/518931908542341121. It was later unblocked.
\(^10\) Weixin is the domestic version of an application Tencent launched globally as WeChat.
\(^12\) See, https://paopao.net/article/199.
organ of the state.17 Lu Wei appears increasingly central to Xi Jinping’s internet strategy, and was appointed in February 2014 to a panel on information technology and security policy which the president himself heads, a role usually played by the premier.18 This high-level committee positions internet development, governance, and cybersecurity as fundamental issues for Xi’s administration, along with national security and economic reform.19

Xi’s renewed focus on cyberspace comes as China lobbies to change internet governance on a global scale. The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization responsible for internet protocol (IP) addresses and URLs, operating with input from nongovernmental stakeholders. In recent years, China has pushed to disempower these nongovernmental groups by transferring ICANN’s regulatory powers to a governmental body, the United Nations International Telecommunication Union.20 The Chinese political system found new ways to suppress internet freedom domestically in 2014, even while technical, commercial, and legal constituents helped sustain it in Hong Kong. More authoritarian influence over digital resource allocation could tip that balance irrevocably in favor of the state.

## Obstacles to Access

China reported 618 million internet users in January 2014.21 Average connection speeds were comparatively slow at 3.2 Mbps.22 Obstacles to access include 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 access to quell social unrest. Nationwide blocking, filtering, and monitoring systems delay or interrupt access to international websites.

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).23 Though the digital divide between urban and rural areas narrowed marginally in 2013, 71 percent of users were based in cities, and more were documented in Eastern China than in the less developed Central and Western regions combined.24

---

Penetration rates vary by province, from Beijing (75 percent) to southeast Jiangxi (32 percent). Overall internet penetration was 46 percent. The Center reported a gender divide of 56 percent male to 44 percent female.

Mobile replaced fixed-line broadband (which has dwarfed dial-up since 2005) as China’s preferred means of accessing the internet for the first time in 2012. By December 2013 the 500 million mobile internet users reported by the CNNIC was more than double the 210 million fixed broadband subscriptions.

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. By 2012, chains had absorbed around 40 percent of cybercafes. More than 10,000 locations closed between 2011 and 2012, and cybercafes provided access for less than 20 percent of internet users in 2013.

Costly, inefficient broadband service helps to account for 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. The same year, an antimonopoly investigation accused state-owned China Telecom and China Unicom of abusing their market dominance to manipulate broadband pricing in the first use of a 2008 antimonopoly law against state enterprises. The telecom giants revised their internetwork pricing structures to allow rivals access to their infrastructure, and customers can now choose from among scores of private internet service providers (ISPs). The MIIT ordered homes constructed within reach of public fiber-optic

---

networks be connected via a selection of service providers from April 2013 onward.37 A “Broadband China” government strategy issued in August 2013 aims to boost penetration to 70 percent nationwide by 2020, 3G mobile internet penetration to 85 percent, and increase connection speeds to 50 Mbps in cities and 12 Mbps in rural areas, with Gbps speeds promised in bigger cities.38 In 2013, however, the average speed in Shanghai was 5.4 Mbps, compared to 2.6 Mbps in the slowest province, Qinghai.39

State-owned China Mobile, China Telecom, and China Unicom dominate the mobile market, but in December 2013 and January 2014, the MIIT issued licenses to 19 companies to provide telecommunications service by leasing network infrastructure.40 The MIIT issued 4G licenses to the three providers in December 2013.41 High prices have slowed 3G adoption in China, especially as some social networks 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.42 In May 2014, the government formally authorized the three major players to set pricing for services according to market forces, resulting in price cuts.43

Despite these signs of liberalization, six state-run operators maintain China’s gateways to the international internet, giving authorities the ability to cut off cross-border information requests.44 All service providers must subscribe via the gateway operators under MIIT oversight.

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 Uighur Autonomous Region—home to 22 million people—after ethnic violence in the regional capital, Urumqi, in 2009.45 Since then, authorities have enforced smaller-scale shutdowns, including one in Xinjiang’s southern Hotan city in June 2013 which affected cellphone service, internet and the messaging app Weixin for several weeks in the wake of a clash between police and locals over the detention of a religious leader.46

In January 2014, analysts said a massive internet outage affecting most of the country may have been caused by censorship technology mistakenly redirecting the nation’s traffic to specific internet addresses instead of blacklisting them. The volume of traffic quickly overwhelmed the addresses, crashing their host servers and effectively shutting down internet service for around eight hours.47

---

38 http://www.miit.gov.cn/n11293472/n11293832/n13095885/15586409.html
Several government and CCP agencies are responsible for internet censorship at the local and national level. The State Internet Information Office was created in 2011 to streamline regulation of online content, punish violators, and oversee telecommunications companies.48 Two regulatory bodies, the State Administration of Radio, Film, and Television (SARFT) and the General Administration for Press and Publications (GAPP), merged in March 2013 to form the State Administration of Press, Publications, Radio, Film and Television.49

Limits on Content

The CCP propaganda department, government agencies and private companies employ thousands of people to monitor, censor, and manipulate content. Routine censorship is reinforced during politically sensitive events or breaking news. Even this manipulated online environment, however, provides more space for average citizens to express themselves criticize the state than any other medium in China.

A range of issues are systematically censored, including independent evaluations of China’s human rights record, and treatment of ethnic minorities and the banned Falun Gong spiritual group.50 Criticism of individuals, policies or events considered integral to the one-party system is tightly controlled, but the nature of that control is subject to change. In June 2013, Sina Weibo briefly stopped banning searches for the “June 4th incident,” instead hiding results that referenced the 1989 military crackdown on student-led protests in Beijing; it also removed the candle emoticon often used to indicate sympathy, and, when users complained, blocked searches for the word “candle.”51 In 2014, censorship intensified in advance of the 25th anniversary of the protests to encompass phrases like “return to Tiananmen.”52 In May, one blog reported that a user-generated encyclopedia hosted by Baidu had entries for 1988 and 1990, but not 1989.53 Yet political discourse can be vigorous online, even about democracy and constitutional government.54 This is partly because leaders redefined democratic governance as “the Chinese Communist


https://en.greatfire.org/blog/2013/may/sina-testing-subtle-censorship-ahead-tiananmen-anniversary-0.


Party governing on behalf of the people” in 2005. But officials also want 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.

At the same time, forums on “constitutionalism” were banned on at least one platform in 2014 after it became associated with a fledgling civic movement, suggesting social movements are perceived as more of a threat than opinion. According to one 2014 study, “even posts that praise the government are censored if they pertain to real-world collective action.”

Censors will downplay civic crusades even at the expense of public health. In March 2014, censorship of protests against a local chemical plant in Maoming may have helped perpetuate disinformation, according to one commentator. Similarly, officials were investigating “rumors” about water pollution in Lanzhou, the capital of Gansu province, a month before they acknowledged it was unsafe to drink.

Names of dissenters with social capital are often censored. Examples during the coverage period include “Tan Zuoren,” when the freelance journalist who investigated schools damaged in the 2008 Sichuan earthquake ended a five year jail term, and “Cao Shunli,” after the human rights activist died in jail. Blocks on “Xu Zhiyong” implemented during the lawyer’s detention for antigovernment protests were lifted to publicize a negative verdict, though a speech he made during his appeal was censored.

In 2013, the trend of targeting influencers broadened to encompass “Big V,” Weibo’s term for VIP users with millions of followers. Hundreds of users were questioned or detained across the country in a government campaign to stamp out rumors, and use of Weibo dropped. Outspoken users had

their accounts cancelled on Weibo and other platforms. Novelist Hao Qun, who writes as Murong Xuecun, told The New York Times all his social media sites were deactivated in May.69

Anti-pornography and anti-rumor campaigns are a longstanding cover for censorship of social and political content. The SIIO shut down more than 100 grassroots news websites between May and June 2013.70 In April 2014, another 3,300 social media accounts were deleted in an anti-pornography sweep.71

The government is not 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.”72 Blacklists periodically leak online, but are not officially published. Censorship decisions are arbitrary, opaque, and inconsistent, in part because so many individuals and processes are involved. There are no formal avenues for appeal. Criticism of censorship is censored.73

In January 2014, a handful of global news websites were inaccessible for two days after they reported the findings of an International Consortium of Investigative Journalism report about elite politicians using offshore tax havens.74 Censorship like this is a result of the automated, technical blocking of foreign websites commonly referred to as China’s “Great Firewall.” In some cases, whole domain names or IP addresses are blocked with an explicit message about illegal content. Other interventions are less visible. Slow speeds characteristic of throttling, which delays the loading of webpages, has also been documented.75

Authorities also use deep packet inspection to scrutinize both a user’s request for content and the results returned for blacklisted keywords. Once detected, the technology signals both sides of the exchange to temporarily sever the connection. This 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.76 Security forces can also monitor who is accessing banned content.77

Filtering is heterogeneous, depending on timing, technology, and geographical region. ISPs reportedly place filtering devices differently, in the backbone and even in provincial-level internal networks, a development that would potentially allow interprovincial filtering.78 The University of Macau’s new

---


73 King, Pan, Roberts “How Censorship in China Allows Government Criticism but Silences Collective Expression.”


77 Villeneuve, Breaching Trust.

campus in southern Guangdong province, meanwhile, advertised unfiltered internet access. However, reports that the same would apply in a special economic zone in Shanghai proved inaccurate. As political upheaval flared in Taiwan and Hong Kong in 2014, censors sought to shut off interaction with the mainland, disrupting mainland access to chat applications like KakaoTalk and LINE those communities used to mobilize, and censoring vocabulary specific to political developments.

Mobile service providers also monitor text messages and delete pornographic or other “illegal” content. Users report receiving blank messages in place of banned keywords, though what content is banned appears to vary.

Select web applications are totally blocked, isolating the Chinese public from an international network of user-generated content. The video-sharing platform YouTube and social media sites like Facebook, Twitter, Google+, and Foursquare are consistently inaccessible, but popular among Chinese users who employ circumvention tools. Document-sharing applications like Google’s cloud storage service, Drive, are also blocked, and other Google applications like Calendar and Translate became inaccessible in June 2014, just outside the coverage period of this report. Domestic internet firms are quick to fill the void, but must prevent banned content from circulating as part of their licensing requirements. Chinese company executives also benefit from political patronage.

Many social media applications produce sanitized versions for the mainland Chinese market:

In late 2013, researchers at the University of Toronto-based Citizen Lab reported that the Japanese messenger service Line automatically censored keywords typed by users who set their country to China while installing the application. Messages containing the banned words would be disabled before sending, and replaced by asterisks when received, the research revealed.

---

Apple removed anticircumvention apps Open Door from its app store in October 2013, and Free-Weibo in December. The company had rejected another app for sharing books that are banned in China in April.

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.

In February 2014, the censorship watchdog nonprofit organization Great Fire said Microsoft’s search engine Bing was censoring results for search terms banned in China, like “Dalai Lama,” even outside China. Microsoft denied intentionally manipulating the results, but internet researcher Rebecca Mackinnon reported that the error was a result of the company’s algorithm sorting content by popularity. The number of users in mainland China accessing government-approved results about the Tibetan spiritual leader caused Bing to reflect the same censorship elsewhere.

In August 2013, Weixin’s international version WeChat suspended the account of a popular overseas Chinese-language web portal that is blocked in China, even on its supposedly uncensored international version.

Instant-messaging services such as Tom-Skype and QQ include programming that downloads updated keyword blacklists regularly. Other companies employ people to delete posts, sometimes before they appear to the public. Experts say staff members receive as many as three censorship directives per day by text message, instant message, phone call, or e-mail. Most of these directives come from local propaganda agents. However, the CCP established party branches in four microblog

---

91 See, http://www.ft.com/intl/cms/s/0/39e02d6c-9d02-11e2-88e9-00144feabdc0.html?siteedition=intl#axzz3KgCeMhgM.
98 King, Pan, and Roberts, “How Censorship in China Allows Government Criticism but Silences Collective Expression.”
company offices in 2012 to improve compliance, according to news reports. 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.

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, was jailed for 10 years 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 paid 483,000 yuan ($78,000) in one year.

Other content has been suppressed by private actors. In June, Beijing-based Caixin Magazine reported that a China Central Television 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 including negative ones about their own performance, according to one analysis.

---

**Microblog vs Micromessage**

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’s Weibo (“microblog”) and Tencent’s Weixin (“micromessage”). 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, which are lost if that post is censored; the feature can also be shut off to prevent posts 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 ten percent of users, while thousands of others were zombie accounts created for marketing.

---

104 “Caixin Report Provides Context for Baidu’s 2011 Censorship of Search Results for “CCTV Baidu.””
or spam. Sina’s efforts to manage Weibo content are well documented. Staff, reportedly 150 of them working 12-hour shifts at a time, delete individual posts or accounts, often with 24 hours of an offending post, but sometimes long after publication; make published posts visible only to the account owner; and personally warn individuals. Hundreds of terms have been automatically filtered from Weibo search results over time.

Weibo was punished with restrictions on some of its functions in 2012 for failing to curb rumors. In November 2013, following the intensified antirumor campaign, Weibo said 1,000 accounts were shuttered for posting false information out of a total 100,000 accounts disabled for harassment and other violations. Activity on the platform dropped an estimated 70 percent. By January 2014, the CNNIC report reported that 38 percent of Weibo users had migrated to Weixin.

In 2014, Tencent reported a combined 396 million monthly active users for Weixin and its international equivalent, WeChat. Users have the option to restrict updates to a closed circle of connections, and can send audio messages that bypass keyword censors, so some activists prefer it. Yet the service still polices political content. In what users described as a “massacre” in March 2014, Tencent’s Weixin closed dozens of accounts, including one run by investigative journalist Luo Changping. Dissidents Hu Jia and Bei Feng both reported their accounts deleted during the coverage period.

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 instructed: “Media that report on the knife attack incident that occurred March 1


at the Kunming railway station must strictly adhere to Xinhua News Agency wire copy or information provided by local authorities. Do not treat the story with large headlines; do not publish grisly photos.¹²¹ In April 2013, regulators instructed journalists operating online not to post articles from overseas websites or independently upload information obtained while reporting.

Since 2005, propaganda units at all levels have trained and hired web commentators to post pro-government remarks and lead online discussions.¹²² They also report users who have posted offending statements, target government critics with negative remarks, or deliberately muddy the facts of a particular incident.¹²³ Coordinated smear campaigns aim to discredit high profile government critics.¹²⁴

These methods are not always effective. Many 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.”¹²⁵

In March 2014, 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 ($1,108).¹²⁶ Government employees also openly engage citizens in online discussions. In October 2013, an opinion monitoring official at the People’s Daily newspaper said that the quantity of posts by government-run and traditional media Weibo accounts had overtaken those by the Big V online personalities.¹²⁷

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 virtual 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 e-mail to subscribers in China with news, instructions on circumvention tech-

nology, 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.

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.128 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 is kept in check, with officials frequently exposed for overspending on entertainment or designer watches, a sign of possible corruption.129 As the public opinion monitoring trend shows, officials do seek to gauge, and are influenced by, the public's response.

The transformative effect of online activism in China is undeniable, and yet the solutions that result from these high-pressure encounters typically fall short of systemic reform or democratic decision making. Consequently, they fail to ensure meaningful accountability.130 Censors intervene if campaigns gain too high a profile or implicate overall CCP governance. In the past year, some NGOs found their ability to fundraise using e-commerce platforms obstructed, including a rural library project which was forced to close in September 2014.131

Mobilization can also have a negative impact. Nationalism and xenophobia are prominent components of Chinese cyberspace, though censorship targeting 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 the mainland, Weibo said 60 percent of microbloggers polled called the action “irrational,” but censored posts that compared it with June 4.132

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 substitute for

---


130 According to one study, censors stopped blocking names 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, “Finish Study Analyzes Keyword Censorship during Mass Incidents,” China Media Bulletin December 13, 2012, http://www.freedomhouse.org/cmb/77_121312#5.


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.”

Software developers, both domestic and overseas, offer virtual private networks (VPNs), which encrypt the user’s traffic and reroute it through a server outside the firewall to circumvent technical filtering. Users tend to adopt these tools at politically important moments when censorship is heaviest, but continue to use them thereafter. In 2011, internet security experts noticed activity indicating that Chinese ISPs may have been testing a new system for identifying the type of encryption indicative of circumvention. In 2012, China Unicom was reportedly cutting connections when it detected VPN usage. Even when not actively disrupted, encryption may attract surveillance. In December 2013, censors disrupted access to peer-to-peer circumvention tool, Lantern. In May 2014, government officials announced plans to mandate inspections of international technology products and services.

Violations of User Rights

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, and state secrets legislation to imprison citizens for online activity.

The legal grounds for these charges was bolstered during the coverage period. On September 9, the Supreme People’s Court and the prosecutorial body, the Supreme People’s Procuratorate issued a j-

---


135 Xiao, “From ‘Grass-Mud Horse’ to ‘Citizen.’”


137 E-mail communication with circumvention tool developer who requested anonymity, June 2012.


140 MacKinnon, “The Shawshank Prevention.”


dietical interpretation “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 digital defamation, as well as online manifestations of other crimes, creating disturbances, illegal commercial activities, and extortion.143 Local officials have detained online whistle-blowers for criminal defamation, which carries possible three-year prison terms “serious” circumstances under the penal code, in the past.144 The new interpretation defined those circumstances as more than 5,000 views or more than 500 reposts on the internet.145 Online messages deemed to incite unrest or protest are also subject to criminal penalties under the interpretation.

The announcement came out of a campaign to curtail protests. The Procuratorate instructed Chinese prosecutors to combat crimes that “disturb social and public order” in June,146 and police around the country detained at least 55 activists between February and August 2013 for participating in collective action.147 Many were formally arrested, notably lawyer Xu Zhiyong on August 2 on charge of disturbing public order.148 When prosecutors outlined their case against him in December, it included three disruptions to “public spaces on the internet” based on the September judicial interpretation, apparently based on the act of uploading photos taken at 2012 civic protests.149 A Beijing court sentenced Xu to four years in prison in April 2014.150 Other online dissidents detained during the coverage period include Huang Qi and Wang Zhenhua.151

The scope of this campaign widened from established political activists to well known online commentators at the Beijing China Internet Conference of August 13-15, 2013.152 The conference established seven baselines, or limits, for bloggers and internet users. Though framed as an attempt to combat rumor, the list began with instructions to respect laws and regulations, the socialist system, and national interest; accuracy came in last.153


145 Human Rights Watch, “China: Draconian Legal Interpretation Threatens Online Freedom.”

146 http://www.chinanews.com/gn/2013/06-19/4947030.shtml


Journalists and international human rights groups estimate that hundreds of internet users were detained in the crackdown.154 On August 23, police detained Charles Xue, a naturalized American businessman with more than 12 million Weibo followers, where he appears as Xue Manzi.155 While he was charged with soliciting a prostitute, state media cited his case as a warning to other Big Vs.156 The connection between the prosecution and his microblogging success was underscored when state TV broadcast two separate confessional interviews with him—one, in August, on his alleged crimes,157 and another in September about his online following. “It’s not right for [popular bloggers] to behave higher than the law,” he said in the broadcast, in which he wore handcuffs.158 The People’s Daily also published his confession.159 Xue was held without trial until his release on medical grounds in April 2014.160

Other outspoken members of the business elite were targeted amid the crackdown, including venture capitalist Wang Gongquan, who was arrested in September for disturbing public order after calling for Xu Zhiyong’s release. He was released in January after police used his testimony in Xu’s trial.161 Billionaire Pan Shiyi, who led social media calls for the government to address air pollution in a major example of successful online activism in 2013, was shown in a CCTV interview in September 2013 apparently designed to pressure him into publicly endorsing the new restrictions for Big V.162

Some individuals were punished for actual rumor mongering, including online marketer Qin Zhihui, who was jailed for three years after confessing to spreading false information.163 One blogger was detained after allegedly fabricating an incident of H1N1 in northern Hubei province.164 Of these cases, some were targeted after publishing muckraking reports. Wu Dong, whose online analysis of official Yang Dacai’s high-end timepieces lead to Yang’s conviction for corruption on Septem-
November 5, 2013, was himself detained for a day later that month.\textsuperscript{165} Investigative journalist Liu Hu was detained in August 2013 and formally charged with defamation in September after publishing allegations of corruption on his microblog.\textsuperscript{166} He was released without trial a year later pending further investigation.\textsuperscript{167}

While observers documented a decline in outspoken posts following a rise in arrests, one detention was less successful in suppressing online activism. Police in Gansu arrested 16-year-old Yang Hui in September for probing the account of a suspicious death at a local karaoke parlor on Weibo. He was released seven days later after web users rallied in his defense and publicized scandal allegations implicating local police.\textsuperscript{168}

As in past years, religious and ethnic minorities faced particularly harsh treatment for online activity. In October 2013, state media reported that 400 people were being investigated in Xinjiang for alleged rumormongering, 110 of whom had been detained.\textsuperscript{169} In January, professor and Uighur rights activist Ilham Tohti was detained in a raid on his Beijing home. He was later charged and indicted with separatism, in part for allegedly spreading rumors, inciting ethnic hatred and conducting separatist activities on a website he founded.\textsuperscript{170} Separatism charges carry a possible death penalty in extreme cases. In September 2014, outside the coverage period of this report, a court sentenced Ilham Tohti to life imprisonment.\textsuperscript{171} At least two Tibetans were reported detained in relation to images of the Dalai Lama stored on their cellphones. Police found one had been sharing the images during a random search of his device; another was additionally accused of expressing anti-China sentiment on Weixin.\textsuperscript{172} One news report said two monks had been jailed for documenting self-immolation protests on Weixin in summer 2013, one for six months, one for a possible life sentence.\textsuperscript{173}

\begin{footnotesize}
\begin{enumerate}
\item[166] Sui-Lee Wee, “China Arrests Journalist Amid Crackdown on Rumors,” Reuters, October 10, 2013, \url{http://www.reuters.com/article/2013/10/10/us-china-journalist-idUSBRE9990B820131010}.
\end{enumerate}
\end{footnotesize}
China

Reporters Without Borders documented a total of 74 netizens in Chinese jails as of August 2014.\textsuperscript{174} Dissident Liu Benqi was sentenced for online expression during the coverage period after his arrest in 2012.\textsuperscript{175} 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.\textsuperscript{176} At least two Uighur website managers, Memetjan Abdulla and Gulmire Imin, were jailed for life in the aftermath of ethnic violence in Tibet in 2008 and Xinjiang in 2009, when local courts imprisoned at least 17 individuals involved in websites that reported on Tibetan or Uighur issues, often in closed trials.\textsuperscript{177}

Though these represent a tiny percentage of the overall user population, the 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.\textsuperscript{178}

Chinese authorities abolished the extrajudicial sentence known as reeducation through labor in November 2013 after domestic calls for reform.\textsuperscript{179} However, individuals can be detained in similarly poor conditions in drug rehabilitation centers and “legal education classes” without trial.\textsuperscript{180} 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, are not known.\textsuperscript{181}

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 main-
tained vague language that is open to abuse by police and security agents. In March 2014, Tan Zuoren, who was jailed in 2009 for publishing research about the collapse of school buildings in the 2008 Sichuan earthquake, was taken to a secret location after his release from prison, instead of being returned to his family. In April 2014, the families of 17 Sina employees responsible for screening the company’s e-publication content were informed they were abroad on business for a month, but a local news outlet reported in May they had been detained as part of the pornography crackdown.

Internet users also risk being held under house arrest. Internet and mobile phone connections are often severed to prevent the individual from contacting supporters and journalists. While there are several cases of long-term house arrest, it can be adjusted arbitrarily over time. Some groups tally the number of dissidents known to be held under house arrest, but there are no statistics showing how many were targeted for online activity.

Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically online as being “invited to tea.” Activists have also been instructed to travel during times of political activity.

Bloggers and activists periodically use the law to defend their right to online expression. In August 2013, microblog user Zhang Guanghong sued police after his repost of content that challenged Communist Party history resulted in a seven day detention and the confiscation of his computer. Many lack the resources or the political will to succeed in legal challenges, but there are occasional successes. In April 2014, a court in Guangdong ordered the local health and family planning commission to re-process a request submitted under open government regulations dating from 2007. The commission had declined to release records about resource allocation from a lawyer based in Zhejiang, who successfully sued for them to reconsider.

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.


184 http://www.infzm.com/content/101017


or misuse, especially since some verification is done through a little-known government-linked contractor.

In 2012, the CCP’s governing 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 portals, bulletin boards, blog-hosting services, and e-mail providers already enforce some registration. The MIIT also requires 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 rules extended regulation to the business sector who must gain consent for collecting personal electronic data, as well as 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 ID to hide their affiliation with the propaganda department. In summer 2014, outside the coverage period of this report, 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.

---


198 Rongbin Han, “Manufacturing Consent in Censored Cyberspace.”

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. One analyst estimated that 50 percent of microblog users had exposed their ID numbers to providers by 2012, simply by accessing the platform from their mobile phone. China’s “second generation” national ID cards—which are administered by police—are required to be digitally embedded with fingerprints in China since the first generation of cards became defunct in January 2013.

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 from Beijing, 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.” In May 2013, a Uighur blogger reported he was unable to join a Weixin page about sport using his national ID number, which identifies his birthplace as Xinjiang; he was only able to register through a Han Chinese friend.

Regulations for the Administration of Commercial Encryption dating from 1999, and related rules from 2006, require a government regulator to approve encryption products used by foreign and domestic companies.

Chinese providers are required to retain user information for 60 days, and provide it to the authorities upon request without judicial oversight or informing the user. In 2010, the National People’s Congress amended the State Secrets Law, obliging telecommunications operators and ISPs to cooperate with authorities investigating leaked state secrets or risk losing their licenses. 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 Public Security Ministry allows in a range of criminal cases, but the wording of the amendment was vague about the procedure for that review.
Privacy protections under Chinese law are minimal. In the words of one expert, the law explicitly authorizes 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.\(^{210}\)

Real name registration is just one aspect of pervasive surveillance of internet and mobile phone communications in place in China. The deep packet inspection technology used to censor keywords can monitor users, and personal text and instant message exchanges have been cited in court documents. One academic study reported that queries for blacklisted keywords on Baidu automatically sent the user’s IP address to a location in Shanghai affiliated with the Ministry of Public Security.\(^{211}\) Cybercafés check photo identification and record user activities, and in some regions, surveillance cameras in cybercafés have been reported transmitting images to the local police station.\(^{212}\) Given the secrecy surrounding such capabilities, however, they are difficult to verify.

As with censorship, surveillance disproportionately targets individuals and groups perceived as antigovernment. Reports citing anonymous government officials noted that a camera grid system known as “Skynet” may have “a camera on every road in Tibet” as part of the effort to contain self-immolations.\(^{213}\) A June 2013 report by Human Rights Watch put these activities in the context of a three-year campaign by 5,000 teams of CCP personnel conducting surveillance throughout the Tibetan Autonomous Region.\(^{214}\) In November 2013, local party chief Chen Quanguo reasserted the party’s commitment to real name registration for web and cellphone users in Tibet.\(^{215}\) Beyond regional flashpoints, the national “Safe Cities” program offers security officials an advanced system for monitoring public spaces across China.\(^{216}\)

China is a global source of cyberattacks, responsible for 41 percent of attack traffic worldwide observed by Akamai in early 2014.\(^{217}\) The survey traced the attacks to computers in China using IP addresses, meaning the machines themselves may have been controlled from somewhere else.

The scale and targets of illegal cyber activity lead many experts to believe that Chinese military and intelligence agencies either sponsor or condone it, though even attacks found to have originated in China can rarely be traced directly to the state. However, 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 February 2013, U.S.-based cybersecurity firm Man-

---

diant traced sophisticated attacks to a military unit in Shanghai. In 2014, the company said that attacks had continued even after public exposure.

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.

Another well-documented tactic is spear-phishing, in which targeted e-mail messages are used to trick recipients into downloading malicious software by clicking on a link or a seemingly legitimate attachment. In a 2012 analysis, the U.S.-based computer security firm Symantec linked the group responsible for the 2010 Google breach—dubbed “the Elderwood gang” after a signature coding parameter—to a series of “watering hole” attacks, in which the hackers lay in wait for a self-selecting group of visitors to specific websites. The targeted sites included defense companies as well as human rights groups focused on China and Tibet; one of the sites was Amnesty International Hong Kong. Most concerning, according to Symantec, were the gang’s frequent “zero day” attacks, which exploit previously unknown vulnerabilities in the source code of programs that are widely distributed by software giants like Adobe and Microsoft. Groups that can pull off these attacks are scarce, since uncovering security loopholes requires huge manpower and technical capability, or internal corporate access to the source code itself. Yet the Elderwood gang “seemingly has an unlimited supply” of zero-day vulnerabilities at its fingertips.

Chinese web users have also been victims of cybercrime. Tibetans, Uighurs and others subject to monitoring are frequently targeted with e-mailed programs that install spyware on the user’s device. Other attacks affect the broader population.

---

Colombia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>n/a</td>
<td>8</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>n/a</td>
<td>8</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>n/a</td>
<td>14</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>N/A</td>
<td>30</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 48 million
Internet Penetration 2013: 52 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- In September 2013, the government announced that it would install internet connections in 100,000 houses for low income families as a means of expanding internet access (see Obstacles to Access).

- In a 2013 court case against Google, a judge ruled that the search engine was not liable for the third-party content to which it linked, establishing a positive precedent for intermediary liability in Colombia (see Limits on Content).

- In June 2013, revelations came to light of a large government investment in a new, real-time surveillance apparatus for monitoring and analysis known as PUMA (see Violations of User Rights).

- In February 2014, allegations surfaced that the Colombian army had engaged in secret surveillance of the FARC peace talks in Havana, Cuba, under Operation Andromeda (see Violations of User Rights).

- In February 2014, the Supreme Court issued its first libel conviction for a comment posted by an anonymous user on a newspaper’s website (see Violations of User Rights).
Introduction

The internet first came to Colombia in June 1994, when a connection was established between Los Andes University and the United States, enabling connectivity to a handful of universities, institutions, and corporations. For the first fifteen years, internet connection in Colombia was primarily limited to these bodies; however, access has been expanding and improving steadily since 2010. Despite this improvement, 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 freely on the internet. While there are occasional cases of content removal, takedowns are isolated rather than systematic and stem mostly from muddy legislation rather than onerous governmental policies.

Although Colombia’s internet atmosphere is largely unrestricted, the country is plagued by violence and impunity, and it is in this environment that internet freedom is exercised. Since 1977, 142 journalists have been murdered and hundreds have been threatened, with little response from the judiciary. In this context, self-censorship both online and offline becomes a prophylactic measure for self-protection, particularly in rural areas where violence and impunity are more pervasive than in cities.

In late 2013 and early 2014, internet freedom issues in Colombia were primarily related to intermediary liability and surveillance scandals. In an instance of the former, the judiciary addressed a case regarding Google’s threshold of responsibility and found that the company was not liable for providing links to third-party content. This stands as a positive decision from a freedom of expression standpoint, especially as there are no set laws governing intermediary liability in Colombia. The media also exposed evidence of irregular surveillance carried out by the military against public officials and political leaders. The most recent scandal concerned unauthorized surveillance of the highly-sensitive peace talks in Havana, which were organized to negotiate an end to the longstanding armed conflict between the government and the Revolutionary Armed Forces of Colombia (FARC). Revelations of illegal surveillance activity during such heightened negotiations revitalized a conversation about ongoing misconduct in the surveillance sector and rekindled concerns about governmental regulation of intelligence.

In recent years, Colombian NGOs—namely the Foundation for Freedom of the Press in Colombia (FLIP), Karisma, Dejustica, and Colinodo—have 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. NGOs have also 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.

Obstacles to Access

Colombia’s main obstacles to internet access stem primarily from socioeconomic factors. Lack of basic utilities and affordable internet access are the chief challenges, and amount to informal barriers to information and communications technologies (ICTs). According to the National Department of Statistics (DANE), 98 percent of Colombian homes have electricity, 96 percent have sanitary service, and 36 percent have local phone connections. In contrast to these figures, the 2013 Human Development Report states that only 11 percent have personal computers.

According to the most recent statistics from the International Telecommunications Union (ITU) Colombia’s internet penetration was measured at 51.7 percent in 2013, compared to 49 percent in 2012 and just 26 percent in 2008. Although broadband service is offered in Colombia, internet access is facilitated primarily by DSL and cable connections. According to a 2014 study from Akamai, Colombia’s average internet speed is 3 Mbps—a figure that places it between Brazil and Argentina in terms of speed. Apart from household use, Colombians access the internet through cybercafes and other public access points, such as libraries, schools, and universities, none of which require identification for use. Local municipalities have also begun offering internet access in public squares and buildings. In 2010, 29 percent of those using the internet outside their homes did so through cybercafes, although the number had dropped to 20 percent by 2012, evidence of an increase in home and mobile connections. Approximately four percent of Colombians still utilize the web from public access points such as libraries and schools.

According to DANE, approximately 38 percent of the population has mobile internet service of some kind, ranging from basic data plans to full access, although official numbers do not specify the proportions. Mobile internet is divided between subscription plans, with roughly 4 million users, and on-demand (or pay-as-you-go) plans, with almost 14 million users. High-speed mobile broadband penetration (3G and above), however, is measured at a rate of only 9 percent.

As in many Latin American nations, there is significant geographical disparity in internet penetration rates in Colombia. While the capital, Bogotá, has a rate of 17 percent, the southern rural departments of Amazonas, Vaupés, Vichada, Guainía, and Guaviare have a penetration rate

---

4 ITU, Time Series by Country—Individuals Using the Internet, 2000-2013, accessed June 15, 2014, [http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx](http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx); Editor’s note: It is worth noting that Colombia’s Ministry of Information and Communications Technology (MinTIC) measures internet penetration at significantly lower rates, coming in at 9.5 percent in 2013. The reason behind such disparity in measurement between the ITU and MinTIC, however, remains unclear. For more on this issue, please see: ICT Ministry sector statics as compared to Colombia’s most recent population census, [http://colombiatic.mintic.gov.co/estadisticas/stats.php?id=48](http://colombiatic.mintic.gov.co/estadisticas/stats.php?id=48)
6 DANE, Basic Indicators on ICT in Colombia, 2011, Press release, July 2012.
of less than 1 percent combined.\textsuperscript{10} Only four to five percent of Colombia's population lives in this region; however, the land accounts for approximately 55 percent of the country's geographical area.\textsuperscript{11} Although many indigenous languages are spoken here, there do not appear to be any 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 rather than Quechua or other local languages.

Digital literacy also presents a substantial obstacle to internet access in Colombia. A 2012 Digital Consumers Survey revealed that 28 percent of those not using the internet cite their lack of computer knowledge as the primary reason. Although this statistic is high, it is worth noting that the number was 48 percent in 2010, evidence that Colombians' comfort with computers is increasing.\textsuperscript{12} Official programs such as Vive Digital (MinTIC) and Colombia Aprende (Education Ministry) have begun breaking down barriers to digital literacy. Vive Digital aims to drive technological progress in Colombia via the encouragement of internet use for job creation and poverty reduction. The project's goals are to expand infrastructure, services, internet applications, and the number of Colombian internet users.\textsuperscript{13} Colombia Aprende, the Education Ministry's platform for the promotion of literacy, also aims to expand the use of digital applications and devices, training some 16,000 teachers across the nation.\textsuperscript{14}

Despite the success of efforts to increase literacy, high prices still pose a challenge to access. The ITU's scale of fixed-broadband prices lists Colombia in 78\textsuperscript{th} place (first place is most affordable; last is most expensive) with an average price of US$18.70 per month.\textsuperscript{15} For comparison, Colombia's minimum legal monthly wage is US$320.\textsuperscript{16} The Private Council for Competitiveness, a national think tank devoted to exploring competition, recommends reducing internet connection fees by 50 percent in order to make access more affordable.\textsuperscript{17}

Colombia's population is segmented into six socioeconomic strata. According to the ICT ministry (MinTIC), strata one and two, the lowest income brackets encompassing almost half the population, have an average fixed internet penetration rate of only eight percent.\textsuperscript{18} In order to remedy this situation, the government is including internet connections in 100,000 government-subsidized

\begin{footnotesize}
\begin{enumerate}
\item ICT Ministry, ICT Trimestral Bulletin: December 2013, accessed February 24, 2014, \url{http://colombiatic.mintic.gov.co/602/w3-article-4992.html}
\item Based on DANE population projection for 2012 and the geographic area of the departments.
\item MinTIC.gov, Vive Digital, \url{http://www.mintic.gov.co/portal/viveditgal/612/w3-channel.html}, accessed July 14, 2014
\item Education Ministry, Colombia Aprende, \url{http://www.colombiaaprende.edu.co/html/home/1592/w3-channel.html}, accessed July 14, 2014
\item ICT Ministry, ICT Trimestral Bulletin: December 2013, accessed February 24, 2014, \url{http://colombiatic.mintic.gov.co/602/w3-article-4992.html}
\end{enumerate}
\end{footnotesize}
houses for low income families.\textsuperscript{19} Although this is a positive step, it remains to be seen whether these families will be able to afford monthly service fees, which do not appear to be included with the houses.

While the aforementioned obstacles are significant, there are no legal provisions imposing 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.\textsuperscript{20} 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 is home to 58 ISPs, and while 89 percent of the market is concentrated in the hands of four companies, there are nonetheless multiple market options from which to choose.\textsuperscript{21} 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 “technological neutrality,” and prioritizes efficient use of infrastructure and access to the use of ICTs.\textsuperscript{22} 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 (MinTIC) 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.\textsuperscript{23} 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. ISPs must also apply for licenses to utilize the spectrum, though there have been no complaints of difficulties or bias with this process.

With six mobile providers, but only two companies—Claro and Movistar—controlling two-thirds of the mobile internet market, the mobile landscape is characterized by greater concentration than the ISP 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.\textsuperscript{24} In 2009, the government declared the dominant position of Claro, subjecting it to \textit{ex ante} (prior) regulation on such issues as pricing and service bundling. The structure of the company, however, remains unchanged.\textsuperscript{25} As with ISPs, mobile service providers must also contribute 0.01 percent of their annual income to Fontic.

\begin{thebibliography}{9}
\bibitem{federico} Public statement of President Juan Manuel Santos, \url{http://wsp.presidencia.gov.co/Prensa/2013/Septiembre/Paginas/20130927_03-viviendas-gratiss-tendran-acceso-internet-ninos-cuenten-igualdad-de-oportunidades-Presidente-Santos.aspx}, accessed February 24, 2014
\bibitem{law2} Law 1341, accessed February 24, 2014, \url{http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913}
\bibitem{decree} Decree 4948 (2009), accessed February 24, 2014, \url{http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=38478#0}
\bibitem{cortes} Cortés, C. “Mobile Internet in Colombia - Challenges and Opportunities for Civil Society: The 2013 Spectrum Auction,” Open Society Foundation.
\end{thebibliography}
Colombia

Colombia’s ICT sector is subject to numerous regulatory bodies, all of which are part of the executive branch of government to varying degrees. The three main regulatory bodies—each of which has little independence—are the ICT ministry (MinTIC), 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 leads the oversight function via MinTIC. The CRC, which is responsible for ensuring efficient service and promoting competition in the telecommunications sector, is then chaired by the minister and formed by three commissioners who are also appointed by the president. The ICT minister then designates the head of the NSA. 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,26 to date, there are no clear examples of executive bias in rulings.

Nonetheless, the Organization for Economic Co-Operation and Development (OECD) recently issued a set of recommendations for improving the autonomy of the various bodies involved in ICT regulation. The OECD’s two principal suggestions were that the CRC develop more independence from Colombia’s central government (the body can make recommendations but cannot currently enforce them), and that MinTIC refrain from regulating the sector, and instead, focus solely on promoting the development and use of ICTs.27

In addition to regulating ISPs, MinTIC establishes public selection mechanisms for mobile service providers.28 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, MinTIC renewed the spectrum licenses of Claro and Movistar for a new 10 year term without major alterations, suggesting that little is likely to change in terms of market dominance in the next decade.29 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.30

Limits on Content

Blocking or filtering of content—other than child pornography—is not common in Colombia. Despite the fact that the country has suffered from a violent conflict between the government, the FARC, and other paramilitary and guerilla groups for over 50 years, there are, perhaps surprisingly, no restrictions on publishing materials about the ongoing conflict online.

While deletion of online content is not common in Colombia, periodic court cases have resulted in judicial orders requiring the removal of specific information found to violate fundamental rights.

---

28 Law 1341 of 2009, Article 11.
29 Resolution 597 of 2014, ICT Ministry.
Recent cases pertaining to content disputes have also determined that intermediaries are not liable for posting links to content in their search results. The most important recent ruling concerned the January 2013 case of Guillermo Martínez v. Google and the daily newspaper El Tiempo. In 1997, El Tiempo reported that Mr. Martínez was part of a mafia group. In 2003, charges against Martínez were dropped, but eight years later, when Martínez searched for his name on Google, the original news still appeared.

In response to Martínez’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. The Court’s rationale was that although “Google offers a search service...[it] is not the party editing or publishing such information and [as such] it cannot assume responsibility for the truthfulness or impartiality of the content to which it links.” While such a ruling is not a substitute for a law governing online content and conduct, it is an important precedent for future cases concerning intermediary liability. The ruling suggests that the responsibility of similar services, such as access providers and content hosts, may be limited and does not extend to the opinions expressed by third parties.

There are no significant records of blocking or filtering of political or social content in Colombia. There are, however, legal rulings and proposed laws that could have such an effect, such as data protection and child pornography regulations containing overly broad language. In one August 2013 case pertaining to data protection and privacy, the Superintendency of Industry and Commerce ordered MinTIC to block the websites Cuidomifirma and Udfirmolarevocatoria because the sites disclosed the personal information of those people backing a motion for the removal of the mayor of Bogotá, Gustavo Petro. MinTIC denied the request, citing a lack of legal and technical capabilities. The administrators of the websites eventually removed the pages in question, reportedly for public relations reasons, thus precluding further debate in this case.

Although it is an important protection mechanism, child pornography regulation in Colombia is vague and has, at times, exerted an overly broad effect, negatively impacting other types of content. Decree 1524 (2002) requires ISPs to undertake technical measures to prevent the online availability of child pornography. Such measures—which include blocking and filtering—can easily be triggered by means of a complaint or an official request, and are executed promptly by ISPs. Under this rule, legal sites such as Cleverbot and Ask.fm have accidentally been blocked at times. Such overreach poses a problem not only in terms of the accidental restraint of legal content, but also in terms of transparency, as there is no appeals process for accidental blocks.

In October 2013, the Foundation for Press Freedom (FLIP) requested that MinTIC explain its process and submit the list of websites blocked due to child pornography complaints. The Ministry replied that such information was classified and that the mechanism was in the hands of the police, closing

---

any avenue for civil oversight or judicial control.\textsuperscript{35} Advocates of internet freedom have suggested that a general constitutional remedy appeal (known as a \textit{tutela}) may be the best way to challenge the standing of opaque criteria and a nonexistent appeals process for censored content.

Although Colombia has regulations that prohibit filtering, the wording is vague and could lead to arbitrary practices. Resolution 3502 (2011) provides that ISPs can make segmentation plans “according to the needs of the segment or the user.” There are no known cases of systematic filtering of text messages or mobile phone content, but mobile service providers offer several kinds of data plans, many of them obscure in terms of the kind of content and applications that can be used and the network management being applied.\textsuperscript{36} Fixed internet service is subject to the same transparency and regulation issues.

Although difficult to measure, self-censorship is a notable problem for journalists in the realm of traditional media— and likely spills over into online media as well.\textsuperscript{37} 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 avoided publishing information due to fear of aggression; 35 percent feared losing their jobs or having their media outlets closed; and 25 percent feared pressure from state actors. The survey also revealed that 57 percent of respondents believe that local government pressures the media with allocation of official advertising. This practice is also carried out by the private sector. Of those who participated in the survey, 60 percent believe that media outlets in their region modify their editorial positions in order to gain political favor.\textsuperscript{38}

Given that financing is often extremely difficult, official advertisement can make a significant difference in an outlet’s long-term existence, a reality that is especially true in provinces and rural settings. According to the aforementioned Javeriana Study, 23 out of 61 online media outlets received advertising revenue. Among them, 14 included official (government) advertisement.\textsuperscript{39} Although objective reporting may be compromised if government funds are essential to the sustainability of a business, the situation in the online environment is much less pronounced than that of traditional media. In the traditional setting, official advertisement facilitates the existence of many outlets, and favorable connections with government officials can be the difference between keeping a media outlet open or watching it close. This is especially true in the Colombian provinces.\textsuperscript{40}

While this landscape also applies to online journals, there are no detailed studies regarding the practices of Colombian journalists on the internet, which is by all means a recent phenomenon in Colombia. A 2012 Digital Media Study published by Javeriana University indicates that there

\textsuperscript{35} Communication 5245, ICT Ministry to Foundation for Press Freedom; See also: Decree 1524 (2002), \url{http://www.alcaldia bogota.gov.co/sisjur/normas/Norma1.jsp?i=5551}, accessed February 25, 2014


\textsuperscript{37} Although there are studies concerning journalists, to date, there are none concerning self-censorship among general internet users.


\textsuperscript{40} Foundation for Press Freedom, “Indirect Censorship Project,” \url{http://www.censuraindirecta.org/web/articulos/publicidad-oficial/reforma-legal/colombia}, accessed February 26, 2014,
are 489 online media outlets, most of which are run by individuals. Keeping these numbers and the national survey in mind, it would be safe to say that online sources of information can be manipulated by the government or a particular partisan interest in much the same way offline sources are; however, such control does not appear to be systematic. 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.

Many professional media enterprises are undertaken in Colombia's largest cities and, in general, the government does not interfere with operations. A wide range of sources of information with different viewpoints is available online. Politics is the main subject of online coverage, followed by regional information, culture, and international news. Some 62 online outlets exist for commentary, with 34 devoted to hyper-local coverage, and an additional 202 publishing municipal information. As the Colombian state does not appear to be censoring online media, none of these efforts requires the employment of proxy servers or other methods to circumvent state censorship. 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 15 websites in Colombia.

The internet is also becoming an important tool for social movements in Colombia. A study from the NGO Somos Defensores (We Are Defenders) indicates that during the first decade of the 21st century, 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. Recent mobilizations organized online, such as peasants’ protests in the countryside and demonstrations against education and health bills, have not yet been assessed in terms of real-world influence.

---


Violations of User Rights

Over the past year, multiple revelations came to light regarding the intelligence agency’s surveillance of ICT communications, sparking broader conversations about privacy and security concerns in Colombia. Additionally, in February 2014, the Supreme Court issued its first libel conviction for a comment posted by an anonymous user on a newspaper’s website.

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 independenc[e]” 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 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).”

While there are no specific penalties in place for libel, defamation, irresponsible journalism, or rumormongering online, cases pertaining to online defamation have occasionally been brought before the court with varying outcomes. In one 2012 case, the Supreme Court acquitted a journalist for insult and slander despite the fact that the complainant was a well-known and powerful politician. Following an appeal from the politician, in March 2014 the Constitutional Court reopened the case; the complainant lost the appeal.

Although this case seemed to have raised the defamation threshold against journalists, establishing further protections for journalistic freedom, one notable February 2014 ruling has called into question the range of legally acceptable online speech and privacy protections. In order to better understand the ruling, it is important to note that Colombia has no restrictions on online anonymity. In February 2014, private citizen Gonzalo Lopez was convicted of libel for insulting a public officer in the online edition of newspaper El Pais de Cali. Lopez, who in 2008 used an anonymous profile to...
Colombia

accuse Gloria Escalante, head of public utility company Emcali, of being both a “rat” and a “thief” in the comments section of the newspaper’s website, was the first Colombian to be convicted of libel for content posted online. Lopez—who was allegedly identified as the author of the anonymous comment by his IP address—was sentenced to 18 months and 20 days in prison and was issued a fine of US$5,200. He has announced that he will appeal the conviction.51

As evidenced by the conflicting rulings in the cases above, Colombia has yet to enact specific regulation for the online environment other than legislation regarding child pornography and cybercrimes such as hacking. Although there are no specific penalties for online libel, if Colombia’s criminal code begins to be applied to the internet, it could negatively impact freedom of expression online. Of potential concern for intermediaries is a provision regarding online publication or reproduction of insults against others, which could result in charges of indirect insult and slander.52 To date, however, there have been no such cases, although the climate surrounding online freedom of expression rulings appears to be shifting.

Prosecution, imprisonment, or detention for ICT activities is quite rare in Colombia. While isolated cases have occasionally been exposed by organizations, there are no records of writers, commentators, or bloggers being subject to imprisonment or fines as a result of posting material on the internet.53 Neither are citizens subject to imprisonment or civil liability for posting, accessing, or downloading material from the internet or for transmitting information via email or text messages.

Colombia has no restrictions against anonymous communication or encryption, and there are no registration requirements for bloggers, cybercafe owners, or users. There are some registration requirements for cell phones—sellers must be licensed with the government and owners are expected to register their phones—however, it is largely possible to have a mobile phone anonymously.54

Apart from the occasional public bidding or contract that sheds some light on the matter, getting an accurate picture of Colombia’s surveillance activities is very difficult. The issue 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 supervise such 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.55

Episodes of illegal surveillance (known in Colombia as “Las Chuzadas”) carried out by intelligence agencies, the army, or the police, constitute an ongoing scandal in Colombia. In 2009, the magazine Semana exposed a secret wiretapping operation carried out by a governmental agency known as the

52 For more on Colombia’s Criminal Code as it may pertain to the online environment, see: http://legismediosinstel.wordpress.com/leyes/delitos-de-injuria-y-calumnia/.
Administrative Security Department (DAS) that intercepted the private communications of journalists, politicians, and NGOs. Although DAS was later disbanded, many of the public officials who staffed the project were transferred to the new federal security agency that replaced DAS—a policy that has engendered concern over the scope of the new agency’s activities.56

In June 2013, reports surfaced that the government was establishing a centralized platform for monitoring and analysis, known as PUMA. The government reportedly invested upward of US$100 million in the platform, which is to become operational by the end of 2014 as a “fundamental tool for criminal investigation to ensure public safety” and, according to official reports, is not to be used as a general intelligence-gathering apparatus. PUMA is intended to provide the government with the capacity to intercept communications in real-time, extending to social media, email, telephone networks, and internet data traffic.57 Following reports about the government’s new surveillance platform, Senator Juan Lozano called on the government for increased transparency and regulation surrounding the country’s surveillance programs. 58 To date, no information on PUMA’s processes or oversight has been released. Because the environment is so opaque, it is difficult to assess the scope of surveillance carried out under PUMA; however, the lack of transparency and oversight raise serious privacy concerns.

In February 2014, Semana exposed another round of wiretappings, this one an illegal operation carried out by the army on government representatives taking part in peace talks with the FARC guerrillas in Havana, Cuba.59 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 guerilla representatives. In addition to conducting illegal surveillance, hackers recruited by the army also forged multiple emails between representatives on both sides of the peace talks.60

The scandal has since escalated. In May, one of the alleged hackers, Andrés Fernando Sepúlveda, was arrested, but was later shown to have been working for the presidential campaign of Oscar Ivan Zuluaga, a frontrunner against President Juan Manuel Santos, rather than the army.61 Given that both surveillance and the peace talks were expected to be contentious issues during the May 2014 presidential election—in which President Juan Manuel Santos won re-election—the involvement of a campaign aid hints at an underlying political market for intelligence information.


57 Daniel Valero, “Policía Podrá Interceptar Facebook, Twitter y Skype en Colombia” [Police Will be Able to Tap Facebook, Twitter y Skype in Colombia], El Tiempo, June 22, 2013, http://www.eltiempo.com/justicia/ARTICULO-WEB-NEW_NOTA_INTERIOR-12890198.html


Colombia

In recent years, NGOs have been increasingly vocal about their concern over Colombia’s surveillance policies. In April 2014, Fundacion Karisma and other Colombian NGOs authored a letter to Colombian President Juan Manuel Santos asking that a commission including NGO representatives be convened to assess and reform the national surveillance apparatus. The president appointed an official to meet with the organizations, and the ICT ministry invited NGO representatives to join the official commission on cybersecurity issues. However, this commission, which is formed by representatives of all public forces and the main governmental agencies, avoided discussions of any intelligence issues related to the scandal.

While intercepting personal communications in Colombia does require a judicial order, 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. Retention and treatment of user data by authorities other than the intelligence agencies has not yet been regulated in Colombia. Monitoring of the radio frequencies used for communication can also be conducted without a judicial order. 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 judicial purposes—which can be used under the attorney general's authorization. A service provider that does not comply with these obligations will face fines and could lose its license to operate.

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, 142 journalists have been murdered since 1977; 64 of these cases have already reached their statute of limitations, meaning that the victims’ families will never see justice. Only 19 of those who committed murder have been convicted, and no masterminds have been brought to justice. Impunity—a pervasive problem in Colombia’s judicial system—is ranked by PAN’s Freedom of Expression and Access to Information Index as one of the gravest threats to overall expression.

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. Prior to his death, Molina received threats and verbal attacks online in response to his activism on social networks and radio on behalf of public interest issues. Although there have been

---

63 Personal testimony anonymous digital security and internet freedom expert in Colombia
65 Law 1621 (2013), Article 17.
67 Decree 1704, Article 7.
no significant advances in the judicial investigation, FLIP has suggested that Molina's online activity may have led to his murder.\(^{71}\)

It is worth noting that although some may be targeted for the online publication of critical commentary on the longstanding conflict or other sensitive issues, there is no broader trend of retaliation specifically for online content in Colombia. This is fairly rare in a climate plagued by violence and impunity, and while such threats may eventually follow online journalists, to date, they have not faced the same level of danger as have print journalists.

In 2009, the Colombian government passed new standards for user privacy and data protection with the adoption of Law 1273, which criminalizes various types of cybercrime, including hacking, illegal interception and use of data, and the distribution and use of malware. Penalties range from 36 to 48 months imprisonment, along with fines.\(^{72}\) After hinting at the growing threat of cyberattacks, in 2011, the government announced the creation of a national cybersecurity sector. In early 2014, following the army's Andromeda 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.\(^{73}\) Colombia then partnered with the Organization of American States (OAS) to develop two bodies—the Colombian Cyber Emergency Response Group (coICERT) and the Cyber Police Center (CCP)—in order to ensure the country's cybersecurity.\(^{74}\)

Although the president recently announced that Colombia is vulnerable to cyberattacks, there are few known cases of technical violence.\(^{75}\) While there have been periodic reports of weak cybersecurity protocols in Colombia, some have suggested that the president's recent focus on cyberattacks and hacking may serve as a means to divert attention and blame from the latest government surveillance scandal rather than as an accurate portrayal of the threat level. While phishing—the stealing of sensitive personal data—appears to be a significant issue in Colombia,\(^{76}\) 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.

---


Cuba

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Free</td>
<td>24</td>
<td>23</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>29</td>
<td>28</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>33</td>
<td>33</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>86</td>
<td>84</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>86</td>
<td>84</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 11.3 million

Internet Penetration 2013: 26 percent

Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- In June 2013, access to Cuba’s new high-speed internet was extended to citizens for the first time, albeit only from designated, censored “cyber points” at prices few can afford (see Obstacles to Access).

- In January 2014, Cuba’s telecommunications regulator, ETECSA, announced the possibility of future mobile internet connections as well as home internet access (see Obstacles to Access).

- In April 2014, revelations of a secret U.S.-installed Cuban Twitter, known as ZunZuneo, strained the already tense relationship between Cuba and the United States (see Obstacles to Access).

- From December 2013 to February 2014, the Cuban government cracked down on opposition surrounding the second annual CELAC summit in Havana, detaining at least 3,000 dissidents and harassing or blocking the mobile phones of others (see Violations of User Rights).
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 20 percent of the minimum monthly wage. Although mobile phone penetration has been 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. Nevertheless, a vibrant community of bloggers has managed to document conditions on the island and transmit information beyond Cuba’s borders.

In recent years, Cuba has exhibited a slight opening to the outside world, although this has not yet correlated to a change in the country’s human rights practices. Some 3,000 opposition and civil society members were subject to detention surrounding the Caribbean and Latin American States (CELAC) summit, hosted in Havana in January 2014. The cell phones of known prodemocracy activists were blocked ahead of the meetings, text messages could neither be sent nor received, and those who attempted to call activists were met with busy signals. A number of dissidents were also detained or placed under house arrest as part of “Operation Cleanup,” an attempt to keep citizens from voicing human rights concerns to CELAC representatives.

Although the government appeared to loosen its restrictions on online media by unblocking a number of blogs in 2011, in 2013 a handful of dissident and critical progovernment sites were blocked once again. Phone numbers associated with the “speak-to-tweet” platform, widely used by activists to publicize human rights violations, were shut down in 2012 and remained disabled as of June 2014. Surveillance has continued on the island, where it has been extended to Cuba’s new “navigation halls.” It is likewise still commonplace in offices, where government-installed software monitors email accounts.

Obstacles to Access

Internet access in Cuba is complicated by weak infrastructure and tight government control. While recent years have seen an expansion in the number of internet and mobile phone users, the ICT sector remains dominated by government firms. Restrictions on private enterprise were eased under the 2012 update of Cuba’s economic model. Although proposed reforms did not initially

---


Cuba extend to liberalization of the communications sector, in November 2013, ETECSA, Cuba’s state-run telecommunications company, announced that it will 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 telephony and internet access. In January 2014, ETECSA also announced it will allow balance transfers on cards between prepaid users.

The possibility of self-employment marks a significant shift in Cuba’s economic policy, as it affords more control to the citizenry and advances the government’s recent trend of loosening restrictions on Cuban nationals. Although the Cuban government began to allow the limited creation of private cooperatives by computer science graduates in 2012, tight internet restrictions, along with prohibitively high computer and software pricing, resulted in a nonexistent official market. While a black market for such commodities does exist, Cuban ICT liberalization was mostly rhetoric prior to the late 2013 announcement allowing private workers to serve as self-employed communications agents.

According to the National Statistics Office, there were 2.6 million internet users in Cuba in 2011, representing 23.2 percent of the population. The latest data from the International Telecommunication Union (ITU) places Cuba's internet penetration at 25.71 percent as of 2013—an increase of less than one percent since 2012, when penetration was measured at 25.64 percent. The vast majority of users cannot access the global internet, but are instead relegated to a tightly controlled government-filtered 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. Experts estimate that approximately 5 percent of Cubans periodically have access to the World Wide Web via government institutions, foreign embassies, and black market sales of minutes by those permitted to have such accounts.

Although Cuba still has the lowest mobile phone penetration rate in Latin America, the number is rising due in part to changes in government-imposed restrictions on telecommunications. According to a study from the ITU, in 2009, 620,000 Cubans owned mobile phones. By the end of 2013, this figure had ballooned to nearly 2 million, or about 18 percent of the population. As the number

---

5 “Aprobada categoría de ‘agente de telecomunicaciones’ para el trabajo por cuenta propia” http://www.etecsa.cu/?page=inicio&sub=agentetelecomunicacion.
of mobile phone users has grown, ETECSA has begun implementing small changes beneficial to users. Between 2011 and 2012, the government reduced the sign-up fee for mobile service by over 50 percent—although at a cost of US$60 it still represents three months’ wages for an average worker. Receiving phone calls from within Cuba is now free, the cost of text messages sent within the country has been reduced from US$0.16 to $0.09, and daytime cellphone rates have been cut from US$0.60 to $0.35 per minute.\textsuperscript{13}

Despite these positive developments, the cost of mobile service is still too high for the vast majority of Cubans. The government’s undeclared policy—viewed as an attempt to attract new funds in hard currency—is predicated on convincing Cuban exiles to pay for these services for their relatives in Cuba. As of January 2014, friends and relatives living abroad were able to use an internet service to pay the phone bills of users living on the island.

Cuba has roaming agreements with 365 carriers in 143 countries.\textsuperscript{14} The island’s mobile network reportedly covers 75 percent of Cuban territory, with further expansions planned.\textsuperscript{15} Most mobile phones do not include internet connections, but it is possible to send and receive international text messages and images with certain phones. Phones that utilize Global Positioning System (GPS) technology or satellite connections, however, are explicitly prohibited by Cuban customs regulations.\textsuperscript{16} Additional restrictions are placed on modems, wireless faxes, and satellite dishes, which require special permits from the MIC in order to enter the country.\textsuperscript{17}

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.\textsuperscript{18} Despite the 2013 connection of a high-speed undersea cable known as ALBA-1, there is still no broadband service on the island, and the limited number of Cubans with internet access face extremely slow connections, making the use of multimedia applications nearly impossible. Despite the high hopes associated with ALBA-1, Cuba’s penetration rate has barely grown since 2012.\textsuperscript{19} It is worth noting that the most significant jump in internet access appears to have occurred between 2011 and 2012—prior to the connection of the high-speed cable—when reported internet penetration rates jumped from 16 percent to nearly 26 percent.\textsuperscript{20} According to statistical findings from Google Analytics, Cuba has the slowest connection speed in the Western Hemisphere and is among the worst in the world.\textsuperscript{21} Access over the intranet is

\begin{thebibliography}{9}
\bibitem{16} See: Cuban Customs Website (Aduana General de la Republica de Cuba): http://bit.ly/1hbJFOL.
\bibitem{17} See: Cuban Customs Website (Aduana General de la Republica de Cuba).
\bibitem{18} For the website of the Ministry of Informatics and Communications see: http://www.mic.gov.cu/.
\end{thebibliography}
similarly slow due to weak domestic infrastructure and the limited extension of access to Cuba’s new high-speed cable.

The Cuban government continues to blame the U.S. embargo for the country’s connectivity problems, saying it must use a slow, costly satellite connection system and may only buy limited space. President Barack Obama eased some aspects of Washington’s prolonged trade sanctions in 2009, however, allowing U.S. telecommunications firms to enter into roaming agreements with Cuban providers and to establish fiber-optic cable and satellite telecommunication facilities linking the United States and Cuba. Official media ignored this important change in the U.S. legal framework, and Cuban leaders reiterated their demand for a complete end to the embargo.

The bilateral relationship was also affected by a 2009 incident that directly touched on the lack of open internet access in Cuba. On December 4, 2009, Cuban authorities arrested Alan Gross, an American independent contractor who was in the country to set up individual satellite-based internet connections as part of a U.S. government–funded project. In March 2011, Gross was sentenced to 15 years in prison for committing an act “against the independence or territorial integrity of the state.” Despite a handful of serious health concerns and a self-imposed hunger strike in April 2014, Gross continues to serve the remainder of his sentence in a Cuban prison.

The volatile relationship between Cuba and the United States took another hit in April 2014, when information was leaked regarding a USAID program to improve connectivity and communications in Cuba. Reports surfaced that the U.S. development agency had created a “Cuban Twitter,” known as ZunZuneo, which attracted some 40,000 subscribers before it was shut down in 2012. News of the program, which the U.S. government has called “secret” but not “covert,” and which was ultimately ineffective given Cuba’s many obstacles to access, has strained Cuban-U.S. relations further, and has given the Cuban government ammunition in its quest to label independent bloggers on the island as “U.S.-funded mercenaries.”

In February 2011, Cuban officials celebrated the installation of a 1,600 km undersea fiber-optic cable laid between Cuba and Venezuela at a cost of approximately US$72 million. The eagerly anticipated cable, known as ALBA-1, was expected to increase data-transmission speeds 3,000 fold, yet no news from the authorities was provided for nearly two years. Due to the prolonged silence, rumors


began to spread that Cuban authorities were reluctant to extend access to the general population for fear of enabling a “Cuban Spring.” ²⁸ In late January 2013, ETECSA announced that the cable had been connected, but noted that opening of the line would be gradual (predictably limited to select government offices at first) and that infrastructure would still be enhanced in order to facilitate widespread use of the new technology. ²⁹ In June 2013, citizens were able to access the internet through connections to the new fiber-optic cable in government-run “navigation halls” (see below).

Prohibitively high costs also place internet access beyond the reach of most of the population. A simple computer with a monitor averages around US$722 in retail outlets, and at least US$550 on the black market.³⁰ By comparison, the average monthly Cuban salary is approximately US$20.³¹ Even an internet connection in a hotel costs between US$6-$12 per hour.³² Only 31 percent of Cubans report having access to a computer, the distribution of which is run by the state-owned Copextel Corporation. Of those with access, 85 percent noted that the computers were located at work or school.³³

In June 2013, Cuban authorities opened 121 government-run internet access points, or “navigation halls,” with 444 computers, marking a small step toward greater connectivity in a country with one of the lowest percentages of internet penetration in the Western hemisphere. According to Cuba’s official newspaper, Gaceta Oficial, members of the public are now able to access national websites for US$0.60 per hour and international sites for US$4.50 per hour—a significant reduction from the previous rate of $6 per hour, but still prohibitive compared to an average monthly salary of US$20. The cost for checking email will remain unchanged at US$1.50 per hour. Users have been pleasantly surprised by the relatively high connection speed (for Cuba)—up to 2 Mbps—as well as access to some web pages once blocked by the government. However, sites such as Radio/TV Marti, the U.S. government broadcaster that transmits to the island, remain blocked.

By paying for government-run internet service directly at cybercafes or purchasing a “Nauta” card (a pass that links to ETECSA’s interface of the same name and can only be used at specific locations), users will be able to access temporary accounts, valid for 30 calendar days as of the date of the first session. They will also be 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.

Despite the improvements in options for access and the reduction of fees, 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

---

²⁹ BBC online, “Cuba First High-Speed Internet Connection Activated,” January 24, 2012, http://bbc.in/V0ggOM.
³¹ Agence France-Presse, “Mobile Phone Use Booms in Cuba Following Easing of Restrictions,” April 24, 2008.
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 dissidence.

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 cybernauts 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.

There are only two ISPs in Cuba: CENIAI Internet and ENET (ETECSA). Both are owned by the state, though Telecom Italia previously held shares of ETECSA. In February 2011, 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. As a result, the telecom company is now completely owned by six Cuban state entities. Cubacel, a subsidiary of ETECSA, is the only mobile phone carrier in Cuba.

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. This regulation extends to 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. Cuban officials, doctors, or trusted journalists and intellectuals can now legally connect to an ISP with a government permit. Approved access to the internet, which is typically restricted to email and sites related to one’s occupation, is granted to doctors, professors, and government officials, whose offices are linked by an online network called Infomed. Home connections are not yet allowed for the vast majority of Cubans.

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. Students at the Latin American School of Medicine in Havana, for example, are reportedly granted only 40 minutes per week of internet access, rendering online research or accessing academic journals infeasible. Students of journalism at Havana University are granted up to 40 MB of data access per month as part of the “Hypermedia Journalism” course.

Despite the many barriers, Cubans still find ways of connecting to the internet through both authorized and unauthorized points of access. Some are 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 (CUC) 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 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.

At times of heightened political sensitivity, the government has used its complete control of the cell phone network to selectively obstruct citizens’ communications. During a March 2012 visit to the island by Pope Benedict XVI and the January 2014 Community of Latin American and Caribbean States (CELAC summit) in Havana, bloggers and dissidents reported that their cell phones were not working. One independent journalist who investigated the situation found that calls were being automatically redirected to a phone number belonging to the Ministry of Interior. All calls from dissidents’ cell phones are monitored and the service is cut regularly to those working as freelance journalists or voicing views the government does not condone via citizen journalism. Such was the case in early summer 2014 for three independent reporters working for the news site Hablemos Press. Having identified the media outlet as a threat, ETECSA reportedly disconnected the cellphones of at least three of its writers, each of whom was also detained for between 24 and 96 hours.

The Cuban government zealously pursues those who violate telecommunications access laws, and government technicians routinely “sniff” neighborhoods with their handheld devices in search of ham radios and satellite dishes. In December 2012, the official newspaper Granma explicitly warned against “counterrevolutionary” and subversive use of illegal nets. In an extensive report entitled “Violations of the Cuban Telecommunications System,” Granma detailed the criminal investigation of two highly profitable cyber-networks illegally using ETECSA’s fixed and mobile market channels. The investigation is still in progress, but the information provided by the MIC and the attorney general alleges that the illegal networks began operating in 2009 and were responsible for a loss of revenue for ETECSA totaling US$3 million. 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 January 2014, the Cuban government announced a handful of changes in international policy and even hinted at the potential easing of telecommunications restrictions. A new port was constructed with a US$957 million investment from Brazil to facilitate international trade; discussions over ending the U.S. embargo on Cuba also heated up in early 2014; and Havana played host to the CELAC summit, which convened the leaders of Latin American and Caribbean states in order to encourage dialogue and establish shared goals for the region.

Although details about changes to telecommunications policy were vague and did not include...
information regarding pricing or technology, representatives announced two exciting possibilities for Cubans over the upcoming year—mobile internet connections and home internet access. Experts speculate that access will extend only to the government run intranet and “Nauta” email accounts. Since December 2013, ETECSA has also been working on “opening” Cuban cellphones—which will likely need to support data services (GPRS) if they are to be used for internet activities. If enacted, such a policy shift could have a significant impact on Cuban citizens’ mobile and internet connectivity.

**Limits on Content**

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. With the exception of unauthorized points of access in old Havana, Voice over Internet Protocol (VoIP) is blocked in Cuba, except from some Wi-Fi hotel connections. Restrictions on email in the workplace have been growing in recent years, and dissident websites and blogs continue to be subject to periodic disabling or blocking. The cost of access to technologies that facilitate information sharing continues to be high; nonetheless, there is a vibrant community of bloggers in Cuba who utilize the medium to report on conditions within the country.

The websites of foreign news outlets—including the British Broadcasting Corporation (BBC), *Le Monde*, and *El Nuevo Herald* (a Miami-based Spanish-language daily)—are readily available in Cuba. The sites of some human rights groups, such as Human Rights Watch and Freedom House, remain largely accessible; however, Amnesty International’s website was recently blocked. For the most part, dissident news websites such as *Payolibre*, and independent journalism sites hosted on overseas servers, such as *Cubanet*, are restricted. The Association for Freedom of the Press (SIAPA) is also blocked, as are the websites of dissident organizations with a presence on the island (such as Damas de Blanco, MCL and UNPACU), which remain inaccessible from government-sponsored youth computer centers, navigation halls, and the like. Revolico, a platform for posting classified advertisements, continues to be blocked, despite the apolitical nature of its content. In August 2013, the government also blocked access to Google, explaining that Cuba is working on the development of a “national browser” along with software to centralize contents. News regarding the national browser has been limited; however, and it remains to be seen whether the application has been completed and is ready for use.

Social-networking platforms such as Facebook and Twitter were recently blocked at some universities and government institutions, but may be accessed—with consistent monitoring but varying reliability—from some cybercafes and hotels. The government has also increased its control

---


44 As reported by a source in Havana who wishes to remain anonymous.

45 For Bitácora Cubana see: [http://cubabit.blogspot.com/](http://cubabit.blogspot.com/); For the website of Asociación pro Libertad de Prensa (the Association for Freedom of the Press) see: [http://prolibertadprensa.blogspot.com/](http://prolibertadprensa.blogspot.com/).

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.”

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. The wording of certain government provisions regarding content regulation is vague and allows for a wide array of posts to be censored without oversight. Resolution 179 (2008), for example, 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.”

Beginning in 2007, the government systematically blocked core internet portal sites such as Yahoo, MSN, and Hotmail. As of 2014, 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 Bitácora Cubana blog and the Voces Cubana 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. The University of Matanzas’ student-run blog La Joven Cuba, which faced difficulties in 2012, became accessible again in mid-2013. Content on Elaine Díaz’s blog La Polemica Digital, which suffered similar challenges, remains available, however blog activity is sporadic. In both cases, the associated bloggers were subject to intimidation, resulting in self-censorship.

Following in the footsteps of other repressive regimes contending with a highly literate and digitally interested populous, the government has also launched its own copycat versions of popular websites, such as Wikipedia, Twitter, and Facebook, and by some accounts, is delaying full connectivity of the ALBA-1 cable until the sites are fully operational so that content can be closely controlled. Although the Cuban government’s faux Facebook site, Red Social, was active for only

51 The site’s most recent activity was a “last post” published in August 2012 accompanied by one more exceptional post in December 2012.
52 In May 2012, Venezuela’s minister of science and technology told media that the cable was operational, but that it was up to the Cuban government to employ it. Some experts reported that internet speeds had improved in the Ministry of Interior or other government offices, adding to speculation that the government is using the cable in part to provide Venezuelan officials with access to Cuban government databases, while deliberately postponing access to the cable for average users. See: “Venezuela: Fiber-optic Cable to Cuba is Working,” Businessweek, May 24, 2012, http://www.businessweek.com/ap/2012-05-24/venezuela-fiber-optic-cable-to-cuba-is-working; Larry Press, “Hard Data on the Idle ALBA-1 Undersea Cable,” The Internet in Cuba (blog), May 22, 2012, http://laredcubana.blogspot.com.es/2012/05/hard-data-on-idle-alba-1-undersea-cable.html.
a brief period in 2011, its 2010 copycat version of Wikipedia, known as EcuRed, was still active as of June 2014, and had even inspired an app. The government’s portable version of EcuRed, known as EcuMovil, became available for free installation on cell phones at JovenClubs (youth centers) beginning in April 2014.

Havana seems to be taking its cues in the field of copycat sites from Beijing, which has successfully prevented access to the most popular global social media sites by directing citizens to closely monitored, censored versions of these platforms. In September 2013, the Cuban government announced the launch of a new “Cuban social network” called La Tendedera, which will be accessible only from JovenClubs and will allow the sharing of texts, photos, and videos, while also offering online chatrooms accessible from public or private rooms. According to the official Union of Journalists of Cuba (UPEC), the birth of the new social network comes “after many failed attempts.”

Another new social media development from the regime comes in the form of a Cuban blogging platform called Reflejos. Built on WordPress, one of the companies that manage some of the most popular online content, Reflejos can be viewed from outside youth centers; however, blogging outside the headquarters of JovenClubs is not permitted. Nonetheless, Cuban journalists and bloggers are optimistic about the potential of Reflejos, given that it presents the opportunity for those whose sites are hosted on foreign platforms to have a voice in Cuba. ETECSA has also announced that intranet users will soon be able to use the microblogging platform El Pitazo, as well as a URL shortening site and hypermedia sites, which may host and manage multimedia content.

In Cuba, the obstacles to sharing information are significant—the majority of citizen journalism is done offline, often by hand or typewriter, and uploaded and published once or twice a week. The financial cost of freedom of expression is also great; the tools that facilitate contribution to media outlets, such as paid internet access cards and international phone calls, are prohibitively expensive and present a major obstacle.

While there is no exact count of blogs produced in Cuba, Blogs Cubanos reports that there are now more than 1,600 blogs, including sites such as Retazos and Convivencia. Independent websites hosted outside the country, such as La Polemica Digital, Havana Times, and Estado de Sats, provide the few who are able to access the net with a much richer and more robust selection of news sources and perspectives than those available from state-run media. Regional radio stations, magazines, and official newspapers are also creating online versions, though these are state-run and do not accept contributions from independent journalists. Some of these official sites recently installed commentary tools that foster discussion and allow readers to provide feedback, albeit censored. Other news sites run by Cuban exiles, such as Diario de Cuba, Penúltimos Días, and Café

---


Cuba

*Fuerte* are now censored at some points but available at others. As censored areas change without warning it is difficult to know where and when such blogs will be accessible on the island.

Unable to completely suppress dissident activity on the internet through legal and infrastructural constraints, the authorities have taken a number of countermeasures, including dominating conversations within the medium itself. The Cuban government maintains a major presence on social networks via “Operación Verdad,” (Operation Truth), its veritable cyber militia of approximately 1,000 trusted students from the University of Computer Sciences (UCI) who were recruited to promote the government’s agenda and to slander dissident bloggers and independent journalists. In February 2013, Yoani Sanchez interviewed blogger Elícer Avila, a former UCI student—and leader of Operación Verdad. Referring to the group as the “kilobyte police,” Sanchez stated that the interview “corroborated” theories that the state security had created blogs to “denigrate and discredit the citizen who criticizes the system.”

During the same month, video of a government training on social media appeared on the internet. In the footage, which was apparently leaked, a Cuban official warns agents of the potential threat that activist bloggers pose, alluding to the possibility that a popular blogger like Yoani Sánchez could organize protests in Havana similar to those that occurred in Iran in 2009. He concludes by saying that the government must respond to these threats.

Despite such grave challenges to freedom of expression, a number of activists and bloggers have persisted in making their voices heard. In recent years, Yoani Sánchez, an award-winning dissident writer and the owner of the popular blog *Generation Y*, has become arguably the most visible figure in an independent movement that uses new media to report on conditions that violate basic freedoms. In addition to being vocal on Twitter (Sánchez had over 600,000 followers as of June 2014) and, increasingly, on the world stage, Sánchez has been hosting Twitter workshops in her home for the past three years, a bold move that has resulted in a crop of hundreds of new Twitter users in Cuba.

In mid-May 2014, following a whirlwind global tour that allowed her to raise awareness of human rights abuses in Cuba and the fight for freedom of information and expression on the island, Sánchez launched the first edition of a new, independent online news site known as *14ymedio* (media begun in the year 2014). Although many expected *14ymedio* to be anti-establishment in nature, Sánchez says that her goal is to provide objective news, allowing Cubans to make their

---


own decisions about current events. Reinaldo Escobar, the site's editor-in-chief and Sánchez's husband, stressed this point, saying that writers for 14ymedio would avoid using politically charged terminology, such as "dictatorship" and "regime."63

In addition to the popularity of independent blogs, young people are increasingly turning to Twitter and mobile phones to document repression and voice their opinions. In a world where internet access is highly restricted, tweeting directly by SMS or a "Speak-to-Tweet" platform offers an alternate avenue for communicating with the outside world. Although associated phone numbers are continually blocked, the speak-to-tweet platform "Hábblalo Sin Miedo" (Speak without Fear) has been proactive in finding new phone numbers in order to enable Cuban residents to call a phone number in the United States and record anonymous messages describing government abuses and other grievances.64 The messages are automatically converted into posts shared via Twitter and YouTube.65 At a cost US$1.10 per tweet, Hábblalo Sin Miedo is expensive; nonetheless, it is proving effective in allowing activists to denounce repressive acts and human rights violations.66

**Violations of User Rights**

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. From December 2013 to February 2014, the Cuban government cracked down on opposition surrounding the second annual CELAC summit in Havana, detaining at least 3,000 dissidents and harassing or blocking the mobile phones of others.

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.67 The penal code and Law 88, known as the "Clamp Law," set penalties ranging from a few months to 20 years in prison for any activity considered a "potential risk," "disturbing the peace," a "pre-criminal danger to society," "counterrevolutionary," or "against the national independence or economy."68 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."69 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


Cuba

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 with photo ID, rendering anonymity nearly impossible.

Resolution 56/1999 provides that all materials intended for publication or dissemination on the internet must first be approved by the National Registry of Serial Publications. 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.

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 17/2008, ISPs are required to register and retain the addresses of all traffic for at least one year. 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. In addition, delivery of email messages is consistently delayed, and it is not unusual for a message to arrive without its attachments.

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, however—a phenomenon that spiked in late 2013 and early 2014.

In November 2013, authorities arrested numerous civil rights activists, including Yoani Sánchez and at least 12 others. Among those detained were Laritza Diversent, an attorney who runs the blog Jurisconsulto de Cuba, and Antonio Rodiles, curator of Estado de Sats. Diversent and many others were released shortly after detention, but Rodiles was held in police custody for over three weeks. As it is very difficult to distinguish between independent blogging and political activism in Cuba, it is impossible to accurately pinpoint which offence triggered the detentions.

Regardless of whether an activist is flagged by the government for online or offline activity, arrests in Cuba tend to increase surrounding key political events and meetings; late 2013 through early 2014 proved no exception to this rule. In December 2013, members of Ladies in White, a group of the wives and mothers of 75 “anti-Castro” dissidents jailed in 2003, took to the streets to demonstrate

against human rights abuses on International Human Rights Day, but were detained before the protest could begin.73

Although most were released within hours, threats and arrests of dissidents and activists spiked significantly surrounding the January 2014 Community of Latin American and Caribbean States (CELAC) summit, which was hosted in Havana. The summit, which convenes the heads of state of member nations, was organized to discuss shared objectives for the region extending to economic goals and a peaceful resolution to the ongoing violence in Colombia between the FARC rebels and the government. More than 3,000 “arbitrary, politically motivated” detentions were reported in the three months surrounding the summit.74 The blocking of hundreds of cell phones owned by activists was also reported in the days leading up to the summit.75

In addition to the increase in detentions, reporters associated with independent online newspapers were also subject to increased harassment in late 2013 and early 2014. In October 2013, three dissident journalists were arrested within 24 hours. Mario Echevarria Driggs, a journalist with the website Miscelaneas de Cuba, was arrested while covering a demonstration in Havana. The next morning, David Aguila Montero, head of the Independent Journalists’ Social Agency (ASPI) was arrested as he left his home. A few hours later, William Cacer Diaz, an independent journalist with the online outlet Hablemos Press, was arrested en route to the newspaper’s headquarters. All three writers were released four days after their arrest, along with Denis Noa Martinez and Pablo Morales Marchan, two additional Hablemos Press reporters who had, at that point, been detained for 24 hours.76

In late May, Hablemos Press was again targeted by the Cuban government. Three of its reporters were detained—and their cellphones were disconnected by state-run ETECSA. A member of the state security also reportedly attacked Roberto de Jesus Guerra, the founder of the site, as he walked to an embassy office to file a story online. Guerra and his wife have also begun receiving anonymous death threats.77

As of May 2014, well-known blogger and writer Ángel Santiesteban Prats, who has been serving a five-year jail sentence on trumped-up charges since early 2013, was still imprisoned.78 The winner of major literary prizes, Santiesteban was arrested in connection with his political views several times prior to his December 2012 trial. Such harassment increased after Santiesteban’s creation of the blog “The Children No One Wanted,” in which he criticized the government. Santiesteban has reportedly

been subject to mistreatment and torture since his five-year imprisonment began. To date, there is no evidence that he will be released early.79

Despite the myriad abuses suffered by dissidents, 2013 brought a notable loosening of travel restrictions in Cuba. As part of immigration reform, bloggers previously denied exit visas, including Yoani Sánchez, Orlando Luis Pardo, and Eliecer Ávila, were allowed to travel abroad. In early 2013, Sánchez, who was finally permitted to leave Cuba after having been denied an exit visa 21 times in the past five years, began an 80-city, 12-country tour, with the aim of bringing awareness to Cuba’s active civil society and blogosphere.80 Her speeches and online efforts have since received significant international attention. According to Ms. Sanchez's new website, 14ymedio, a cadre of Google executives visited the island in June 2014 “to promote the virtues of a free and open internet.”81

---

Ecuador

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>甄别到访问 (0-25)</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>内容限制 (0-35)</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>用户权利侵犯 (0-40)</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>37</td>
<td>37</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>人口：</td>
<td>15.8 million</td>
</tr>
<tr>
<td>互联网渗透率 2013：</td>
<td>40 percent</td>
</tr>
<tr>
<td>社交媒体/ICT应用被封锁：</td>
<td>No</td>
</tr>
<tr>
<td>政治/社会内容被封锁：</td>
<td>No</td>
</tr>
<tr>
<td>博主/ICT用户被逮捕：</td>
<td>No</td>
</tr>
<tr>
<td>2014年新闻自由状况：</td>
<td>Not Free</td>
</tr>
</tbody>
</table>

关键发展：2013年5月－2014年5月

- 在2013年8月，厄瓜多尔政府推出了一个全球性的倡议，称为FLOK社会，旨在帮助国家从石油为基础的经济转向信息为基础，开放知识社会（见甄别到访问）。

- 厄瓜多尔通讯有机法，于2013年通过，开始在2013年底和2014年初实施，为传统媒体的控制铺平了道路，这些媒体拥有在线存在（见内容限制）。

- 在公民社会组织的持续呼吁下，政府撤销了厄瓜多尔新的刑法（Código Orgánico Integral Penal）中的第474条，该法将合法化所有互联网交易的监控（见用户权利侵犯）。

- 准备黑客、网络攻击和骚扰事件在2013年底和2014年初增加，包括高官之间的电子邮件拦截和对独立博主的威胁（见用户权利侵犯）。

- 厄瓜多尔政府的有机法，于2013年通过，开始在2013年底和2014年初实施，为传统媒体的控制铺平了道路（见内容限制）。

- 在公民社会组织的持续呼吁下，政府撤销了厄瓜多尔新的刑法（Código Orgánico Integral Penal），该法将合法化所有互联网交易的监控（见用户权利侵犯）。

- 准备黑客、网络攻击和骚扰事件在2013年底和2014年初增加，包括高官之间的电子邮件拦截和对独立博主的威胁（见用户权利侵犯）。
Introduction

Ecuador, a relative newcomer to technological development among Latin American nations, has witnessed substantial improvement in internet access over the past three years. In October 2013, the government’s Institute for Higher Learning (IAEN) launched a global initiative known as Free/Libre Open Knowledge (FLOK) Society dedicated to paving the way for Ecuador to transition away from an extractive, oil-reliant economic model toward a model based on open knowledge.¹ FLOK aims to promote economic prosperity via the creation of a dynamic and innovative society, wherein knowledge and technology are available to all.² Despite such venerable ambitions, the status of internet and press freedom in Ecuador has been highly paradoxical in recent years. While the state guarantees privacy of communications, allegations of state surveillance cast doubt on the reliability of such guarantees.

In June 2013, Ecuador’s controversial Organic Law on Communications was passed. Human rights organizations have feared that the law, which utilizes vague wording, arbitrary sanctions, and the threat of civil and criminal penalties, will stifle critical voices and halt the spread of information that discredits officials, even when such information is supported with evidence.³

In 2013 and 2014, the Ecuadorian government introduced a handful of proposals concerning regulation and control of the internet and was met with increased opposition to potential restrictions from a newly dynamic civil society coalition. On the heels of the June 2013 passage of the communications law, activists from Usuarios Digitales, the government-sponsored FLOK Society, and the Internet Libre collective, lobbied against—and defeated—the broad surveillance provisions proposed under Article 474 of the new penal code (Código Orgánico Integral Penal or COIP).⁴ Had Article 474 been approved, it would have forced internet service providers (ISPs) to record all user activity for six months. Due in large part to civil society action, however, the new penal code was passed in November 2013 without Article 474.

Over the past year, Ecuador has been the focus of some international media coverage regarding the Edward Snowden surveillance leaks. Snowden’s revelations about governmental espionage and privacy violations catalyzed a global debate regarding state surveillance policies—one that grew to encompass Ecuador after President Correa extended an offer of asylum to Snowden. In June 2013, Foreign Secretary Ricardo Patiño reiterated Ecuador’s stance, stating that the country would be a safe haven for Snowden if he were able to reach Ecuadorian soil.⁵ Similarly, in August 2013, the Ecuadorian government released a statement reaffirming its 2012 offer of asylum to Julian Assange, the WikiLeaks founder who had, at that point, been holed up in the Ecuadorian embassy in London for over a year.⁶ Despite its positive stance toward foreign whistleblowers, however, the Ecuadorian

government has a contradictory history of attempting to suppress criticism of political leaders within its own borders (see “Limits on Content” and “Violations of User Rights”).

**Obstacles to Access**

Although it is still developing, Ecuador’s information and communications technology (ICT) sector has experienced tangible growth in recent years due in large part to government efforts to expand access, such as Ecuador’s “Digital Strategy 2.0” plan, intended to extend internet connectivity to 50 percent of households by 2015. As of 2013, internet penetration in Ecuador was measured at 40.3 percent, a notable increase given that penetration was just below 30 percent in 2010. According to a first quarter 2014 report from Akamai, Ecuador’s average internet speed is 3.3 Mbps.

Ecuador has 35,111 kilometers of fiber-optic cable and the government is working to expand internet services across the country so that the technology can be used as a tool for national development. As of September 2013, the government had installed over 1 million network access points as part of its national telecommunications growth strategy. Ecuador has approximately 22 internet service providers (ISPs), three of which—ETAPA, GrupoTvCable, and CNT—offer national coverage. Of all Ecuadorian ISPs, ETAPA and GrupoTvCable hold the greatest percentage of market share. Speeds of 2 Mbps cost an average of US$20 per month, whereas a 5 Mbps subscription can be found for US$40-50 per month. In some places, 10 Mbps subscriptions are available at a rate of approximately US$60 per month. Under a provision prioritizing essential technology, computers, which range from approximately US$800 to $1000, are tax-free when imported from other countries. As compared to an average wage of US$318 per month, however, computers are not easily affordable. For those fortunate enough to own computers, there are multiple internet subscription options, ranging from dial-up pay-per-minute plans to cable and satellite connections. Broadband (commonly used in urban zones) and satellite connections (often used in rural areas) have become increasingly popular in recent years, eclipsing dial-up plans.

Ecuador is also home to an active contingent of mobile phone users. With over 17.5 million mobile

---


Ecuador subscriptions in 2013, the country has a mobile penetration rate of 111.5 percent—meaning that some individuals have more than one mobile phone—a marked increase from 2011, when mobile penetration was measured at 47 percent. 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.

Ecuador is home to three mobile service providers: one state-run operator, CNT, and two private providers, Claro (CONECEL) and Movistar (OTECEL). Claro holds nearly two-thirds of active cellular accounts, followed by Movistar with approximately one-third, and finally, state-run CNT, with less than two percent of subscribers. Despite their popularity, the Ecuadorian government classifies mobile phones as luxury items. In addition to being excluded from the tax exemption extended to computers, 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.

By late 2013, Ecuador had begun making efforts to encourage greater civic participation on issues related to internet freedom and privacy. The launch of FLOK Society and FLOK’s November 2013 “Minga-tec” event opened a much-needed public debate about digital privacy and started a conversation about the relationship between government and civil society within Ecuador. Minga-tec brought global activists and researchers together to promote open source technology and to discuss freedom of speech issues such as global surveillance practices. FLOK Society aims to make Ecuador’s “knowledge revolution” socially, ecologically, and economically sustainable following the country’s stated “principles of good living” (Plan Nacional para el Buen Vivir). These include: strengthening democracy and equality; improving quality of life; strengthening national identity, human rights, and environmental sustainability; and ensuring sovereignty and peace.

In February 2014, the National Secretary for Higher Education, Innovation and Technology launched the region’s first wiki legislation project (WikiCOESC+i). This freely accessible site allows citizens of Ecuador and other nations to propose changes to the Organic Code for Social Economy of

---

Knowledge and Innovation. The goal of the Code is to design a framework for the “inclusive and democratic” development of an open knowledge society, “based on the intensive use of infinite resources.” It remains to be seen how involved the public will become in shaping the new body of law; nonetheless, the government’s provision of an open forum for commentary and proposal offers an innovative avenue through which to encourage civic participation.

Over the past two years, Ecuador has shown improvement in extending internet access to rural areas via Infocentros and Mobile Classrooms (Aulas Móviles), two programs facilitated by the Ministry of Telecommunications (MINTEL). Ecuador’s state-run Infocentros—networked community centers that began to be installed in June 2012—offer internet access in 489 parish communities, and also provide equipment to 7,541 students throughout the country. An additional 387 Infocentros are slated to open in late summer 2014. 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 May 2013, MINTEL received an award from the International Telecommunication Union (ITU) in recognition of the success of its Mobile Classrooms Project. To date, the number of people using Infocentros is over two million nationwide.

In addition to Mobile Classrooms and Infocentros, in rural areas, cybercafes, which generally provide internet access at a rate of US$1 per hour, are often relied upon. Such establishments face the same requirements as other businesses, including registering with the government. In order to utilize the services provided by cybercafes, the national secretariat of telecommunications, SENATEL, requires that users register with the following: 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 SENATEL and the superintendency of telecommunications, SUPERTEL. 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.

Ecuador’s backbone is not highly centralized. 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, each of which can complicate their attempts to enter the market. Private ISPs sometimes engage in bandwidth throttling (the intentional slowing down of internet service) to specific sites when excessive amounts of bandwidth are being consumed.

23 Secretaria de Educacion Superior, Ciencia, Tecnologia e Innovacion, Código Orgánico de Economía Social del Conocimiento e Innovación [Organic Code for Social Economy of Knowledge and Innovation] Accessed April 21, 2014, http://coesc.educacionesuperior.gob.ec/index.php/C%C3%B3digo_Org%C3%A1nico_de_Econom%C3%ADa_Social_del_Conocimiento_e_Innovaci%C3%B3n
24 Secretaria de Educacion Superior, Ciencia, Tecnologia e Innovacion, Código Orgánico de Economía Social del Conocimiento e Innovación [Organic Code for Social Economy of Knowledge and Innovation] Accessed April 21, 2014, http://coesc.educacionesuperior.gob.ec/index.php/C%C3%B3digo_Org%C3%A1nico_de_Econom%C3%ADa_Social_del_Conocimiento_e_Innovaci%C3%B3n
27 AEPROVI, general information available at: http://www.aeprovi.org.ec
It appears as though Ecuadorian ISPs utilize this strategy for traffic management rather than for censorship; however, they are not transparent about such restrictions and there are likewise no laws to protect against preferential treatment of certain sites in times of high traffic.

Ecuador’s state regulatory agency is called the National Telecommunications Council (CONATEL). It is part of the Telecommunications Ministry, the head of which is nominated by the president and also serves as the head of CONATEL, a process which demonstrates close alignment with the executive body. In July 2012, CONATEL issued the Telecommunication Service Subscribers and Added Value Regulation Act. Internet subscribers have taken issue with some of the act’s main provisions, namely, the granting of authority to CONATEL to request users’ IP addresses without a court order (Article 29.9).

**Limits on Content**

In recent years, Ecuador has seen an increasingly controlled media climate—both in print and online media. Although 2013 marked the beginning of a dialogue between a diverse array of social actors and public officials regarding freedom of access legislation and internet governance, state regulatory bodies remain organized in such a way as to have little independence from the executive branch, a factor which compromises transparency and negates the possibility of an independent appeals process for citizens wishing to challenge restrictions on ICT access or content.

While there have been no widespread instances of blocking or filtering of websites or blogs in Ecuador, restraint of political and government-related content is common, both in print and increasingly online. Attempts to censor statements made in times of heightened political sensitivity have also been witnessed, either via letters from the executive branch demanding that editors or website administrators delete content or via the overly broad application of copyright protection principles to content critical of the government. The former has involved news outlets that have allowed readers to post comments critical of the Correa administration on the comments sections of their websites. Following letters from the executive and court proceedings, in 2012, the comments sections of popular media outlets *La Hora* and *El Comercio* were each disabled indefinitely.

The use of copyright infringement claims as grounds for the removal of critical content has often
involved Spanish copyright infringement firm Ares Rights. The firm has come under fire for its issuance of takedown notices on behalf of the Ecuadorian government, forcing the removal of a 2012 documentary about President Correa on grounds of copyright infringement for the use of the president’s image, and catalyzing censorship of the film “Intag Indefensión.”34 Clips of the film, a politically sensitive documentary produced and directed by renowned filmmaker Pocho Álvarez, were posted on YouTube and Vimeo in late 2013. Ares Rights removed the content, which documents the impact of mining in the ecologically and socially vulnerable region of Intag, in response to complaints from government-run public television station ECTV.35 Although the video was later reposted on a handful of sites with the original content, including YouTube, where it is currently available,36 it is worth noting that its removal was not an isolated incident, but was part of at least one dozen takedowns of photos, videos, and documents that painted the government in an unflattering light.37 In April 2014, the Twitter account of politically active blogger Diana Amores was also taken down by a copyright infringement claim issued by Ares Rights. Amores’ offence was retweeting a letter from the president to the people of Quito during local elections in January. Amores’ account was restored 24 hours after the takedown, after Twitter’s evaluation of the copyright infringement law concluded that it had been used incorrectly.38

The Board of Communication Control (CORDICOM or Consejo de Control de la Comunicación), which regulates media content, has played a pivotal role in increasing self-censorship primarily by prescribing high penalties for private citizens, journalists, and media companies that do not comply with the vague and overly broad rules for online content dictated in the country’s highly controversial June 2013 Organic Law on Communications. As the institution that founded the Superintendence of Information (Superintendencia de la Información), CORDICOM is responsible for the rules and penalties for online media platforms, as part of the Communications law.39

In addition to tasking website owners with “ultimate responsibility” for all hosted content, prescribing arbitrary sanctions for unbalanced reporting, and banning “media lynching”—an accusation often applied to investigative reporting in Ecuador,40 the Organic Law on Communications also grants the Superintendency the power to audit, intervene, and control

36 Poncho Alvarez’ documentary Intag Indefensión was reposted on the following sites: exTrends, http://www.extrends.co/video/intag-indefension/10579/; Conflictos Mineros (the observatory of miners’ conflicts) http://www.conflictosmineros.net/biblioteca/videos/video/latest/intag-indefension; and also, by the filmmaker himself on YouTube, http://www.youtube.com/watch?v=6gIaK3Atc_s
38 The timeline of Diana Amores’ account is posted on her Facebook and Twitter pages: @Diana_Amores; facebook/DianaAmores
all information and media, as well as to enforce regulations governing information and communications. Although a promising step was taken in January 2014, when secondary legislation (Article 2) explicitly excluded individual expression on social media and personal blogs from regulation by the Superintendency, CORDICOM maintains the power to enforce all rulings and to further interpret the rules. A handful of conflicting articles in the Communications Law further cloud the environment: although Article 2 seems to protect freedom of online speech, Article 3 extends control of content by CORDICOM to “all media with an online presence,” which could easily negate the positive implications of the exclusionary clause in Article 2. While such contradictory regulation renders online expression legally precarious, the practical application of these powers has yet to be witnessed, leaving the legal status of personal expression online uncertain.41

Although it has been a bit slow to catch on, social media use is growing in Ecuador. As of June 2013 the country claimed nearly 6 million active Facebook users and 2.5 million Twitter users42—for point of comparison, Ecuador’s population was estimated to be 16.7 million as of July 2014.43 Access to blogs and social media platforms such as Facebook, Twitter, and YouTube is generally free and open in Ecuador; however, the government has periodically made announcements about its ability to monitor and regulate social networks. To date, it does not appear to be exercising this power, which would present an infringement on user privacy.44

The Ecuadorian government has also been accused of manipulating conversations online via progovernment 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.45 Although difficult to prove, evidence of internet trolls who post government propaganda and slander critics online has also been apparent surrounding electoral campaigns. There is no legal mechanism in place to combat such activity, but to date the threat of being discredited by trolls does not appear to have deterred citizens from participating in online debate.

Although tensions remain high, online activism is fairly robust. Sporadic threats against independently minded bloggers and activists did little to deter Ecuadorians from taking to the internet to voice their opinions in the months leading up to the February 2014 municipal elections.46 Social media sites hosted online protests, and platforms such as Twitter fostered political debate, allowing citizens to voice their opinions on sensitive topics away from the scrutiny and control of

41 The entire secondary law can be downloaded at the Council of Communications: Cordicom: [link]
42 El Comercio, “Facebook es Aún Lo Más Visto en Ecuador” [Facebook is Still the Most Visited Site in Ecuador] June 2, 2013, [link]
44 Website of CONATEL (National Telecommunications Council), [link]
Ecuador

authorities. 47 In a surprise turn, President Correa’s Alianza Pais party lost the major posts in the largest cities. 48 There appears to be a correlation between the unexpected electoral results and the political leanings of the new internet-influenced generation. Growing internet access has nurtured a generation of politically involved urban youth that mistrusts traditional media and seeks an open and more diverse society.

Over the past year, environmental, ecological, and human rights organizations have been struggling to bring international attention to the plight of indigenous peoples and biodiverse areas being stripped of their natural resources by a government plan to increase revenue. The government, which is intent on suppressing negative news about its extraction of natural resources and its infringement on the lives of the protected peoples of the Amazon, has resorted to online and offline tactics to silence and discredit critics.

One online campaign to bring attention to the plight of the Yasuni, an indigenous group threatened by government-led excavation projects, managed to mobilize social and political actors worldwide. Online protests helped the Yasuni movement collect more than the requisite 500,000 signatures needed for a referendum to stop the oil drilling in the Yasuni area. By early May, however, the government had dismissed half of the signatures due to “format nonconformities” such as using the wrong color of ink. The remaining 360,000 petition signatures deemed acceptable were too few in number to force a referendum. 49

Violations of User Rights

Ecuador has long held an ambivalent attitude toward media, characterized on the one hand by positive development strategies to extend ICT access across the country, offers of asylum to prominent and controversial freedom of information advocates Julian Assange and Edward Snowden (both men face criminal charges in at least one country), and pronouncements about the importance of freedom of speech. These highly visible maneuvers stand in stark contrast with contentious interactions with journalists, increasingly stringent media laws and penalties, mandatory identification and registration requirements for the purchase of mobile phones, and attempts at expanding surveillance of private citizens—while denouncing the vast surveillance carried out by the U.S. National Security Agency (NSA) on American citizens. 50

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

47 María José Calderón, Democracia y Participación Electoral, Cuadernos de Promoción Electoral, [Democracy and Electoral Participation, Electoral Promotion Papers], Instituto de la Democracia, November, 2013
49 The full report can be seen at: http://www.elcomercio.com/politica/CNE-yasunidos-consultapolular-Yasuni-firmas-informevidico-descarta_0_1134486737.html; the Twitter account of yasunidos had high profile advocates such as film stars and politicians campaigning globally; see: @yasunidos, http://www.yasunidos.org/
freedom of expression (Article 384).\textsuperscript{51} However, a discretionary loophole in Resolution TEL-477-16-CONATEL-2012 grants ISPs a wide margin for the implementation of “actions they deem necessary to the proper administration of the service network,” and by extension, threatens net neutrality.\textsuperscript{52} In July 2012, Ecuador’s Ministry of Telecommunications issued a resolution (the Telecommunication Service Subscribers and Added Value Regulation Act) establishing a framework for ICT user rights and the regulation of ISPs. Among its provisions are articles stating that telecommunications is considered a “strategic sector” by the Ecuadorian government, and that the state is tasked with the “administration, regulation, control and management” of such technologies, while also being responsible for ensuring that the public has access to ICTs. Article 14 further establishes a state guarantee of privacy and security for users, prohibiting third party interception of communications.\textsuperscript{53} Despite such positive provisions, however, Article 29.9 of the same act authorizes CONATEL to track IP addresses from ISP customers without a judicial order.\textsuperscript{54} While there are no specific laws criminalizing online content, standard defamation laws apply to content posted online.\textsuperscript{55} Lawsuits have been filed against digital news sites for comments critical of the current administration, and calls for investigations into Twitter users who post content critical of the government have been levied by governmental authorities, including President Correa.\textsuperscript{56}

In December 2013, President Correa announced that his email had been intercepted by two members of his administration: representative Cléver Jiménez (sued by the president in 2011 for libel and under fire again in 2013 for criticizing the president’s alleged purchase of advanced surveillance equipment) and opposition delegate Fernando Villavicencio. After raids on their offices, they were charged with high-level espionage. Following the expulsion of Cléver Jimenez from the National Assembly, he was processed and charged under a separate defamation case.\textsuperscript{57}

In the wake of the aforementioned arrests, in early 2014 the popular humorist Bonil published a cartoon in the newspaper \textit{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 \textit{El Universo} were charged with violating provisions of the Organic Law

---

\textsuperscript{51} MINTEL, “Autoridades del MINTEL se reunieron con usuarios digitales” [MINTEL Authorities Met with Digital Users], Ministerio de Telecomunicaciones y Sociedad de la Información, August 13, 2012, \url{http://www.telecomunicaciones.gob.ec/autoridades-del-mintel-se-reunieron-con-usuarios-digitales-2/}.

\textsuperscript{52} See Article 15.6 of CONATEL’s Telecommunication Service Subscribers and Added Value Regulation Act: \url{http://www.elcomercio.com/seguridad/lueces-ordenan-Luluncoto-transmita-sociales_0_852514906.html}.

\textsuperscript{53} See Article 14 of CONATEL’s Telecommunication Service Subscribers and Added Value Regulation Act: \url{http://www.elcomercio.com/seguridad/lueces-ordenan-Luluncoto-transmita-sociales_0_852514906.html}.

\textsuperscript{54} Carlos Correa Loyola, “Carta Impresa a Domingo Paredes, Presidente del CNE, sobre Intención de Regular las Redes Sociales” [Printed Letter to Domingo Paredes, President of CNE, about the Intention to Regulate Social Networks], Bitácora de Calú (blog), October 18, 2012, \url{http://bit.ly/18l0dBH}.

\textsuperscript{55} Asamblea Nacional de Ecuador, “Constitución del Ecuador” [Constitution of Ecuador], Asamblea Nacional de Ecuador, October 20, 2008, \url{http://www.asambleanacional.gob.ec/documentos/constitucion_de_bolsillo.pdf}.

\textsuperscript{56} \textit{Ecuador Times}, “Rafael Correa Asked the SENAIN to Investigate Twitter Accounts,” \textit{Ecuador Times}, January 25, 2013, \url{http://www.ecuadortimes.net/2013/01/25/rafael-correa-asked-the-senain-to-investigate-twitter-accounts/}.

\textsuperscript{57} Jimenez and two of his advisers were charged for public accusations made against the President in 2011 regarding the events of September 30, 2010. He has sought refuge since April within the Quechua community of Sarayaku in the rainforest region. Updates on the case can be found at the government’s journal el PP Verdadero and El Telégrafo at independent newspaper \textit{Diario Hoy}, \url{http://www.hoy.com.ec/noticias-ecuador/clever-jimenez-se-confiesa-en-el-umbral-de-la-carcel-603113.html} and \textit{El Comercio}, \url{http://www.elcomercio.com/politica/sarayaku-amazonia-clever_jimenez-rafael_correa-Alexa_0_1128487204.html}. For international news: Rosie Gray and Adrian Carrasquillo, “Ecuador Defends Domestic Surveillance,” Buzzfeed, June 27, 2013, \url{http://www.buzzfeed.com/rosiegray/ecuador-defends-domestic-surveillance}. Further information about the police uprising on September 30 can be found at: \url{http://www.elcomercio.com/tag/30s.html} The UN resolution: \url{http://www.elcomercio.com/politica/Mision-ONU-dice-democracia-peligro_0_631136987.html}. 
on Communications.\textsuperscript{58} Under Article 11 of the law, which states that all content without proper verification will be fined, Bonil and \textit{El Universo} were each sentenced to pay US$90,000 to the Superintendency of Information. Bonil was also ordered to issue a formal correction of his cartoon, and \textit{El Universo} was fined an additional two percent of its billings for the three months prior to the verdict.\textsuperscript{59} 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 the government with an overly polite rendition of the raid that made light of the request to formally correct his cartoon.\textsuperscript{60}

In 2013, Ecuador was witness to increased proposals for regulation and control of the internet—along with increased opposition from a newly dynamic civil society coalition. Neither anonymous nor encrypted communications are prohibited in Ecuador; however, an article proposed in October 2013 threatened online anonymity. Four months after the June 2013 passage of the Organic Law on Communications, the National Assembly attempted to pass a new penal code (COIP) containing an Article (474) which would have greatly reduced online anonymity and broadened surveillance of ICT users.\textsuperscript{61}

In response, the internet activist organizations Usuarios Digitales, Apertura Radical, and Asociación de Software Libre del Ecuador launched a campaign on social media under the hashtag #InternetLibre to lobby against Article 474’s proposed surveillance provisions.\textsuperscript{62} 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. Cybercafes would also have been required to install surveillance equipment in order to record video footage of customers.\textsuperscript{63} Due in large part to civil society action, Article 474 was removed before the new penal code was passed in November 2013.

While the deletion of Article 474 is a positive step, in recent years a number of international websites have reported on the Ecuadorian government’s secret acquisition of a biometric surveillance system. The platform, allegedly installed by Russian company Speech Technology Center, is reportedly capable of facial and voice recognition.\textsuperscript{64} Documents have also surfaced detailing attempts to purchase surveillance drones from overseas contractors. The government has defended its right to conduct surveillance in criminal investigations, but has said that it does not engage in such activities

\textsuperscript{58} The corrected version had replies in most newspapers in Ecuador and the region; http://www.hoy.com.ec/noticias-ecuador/bonil-rectifica-caricatura-600290.html; Spain: http://internacional.elpais.com/internacional/2014/02/05/actualidad/1391639841_911785.html; Colombia: http://internacional.elpais.com/internacional/2014/02/05/actualidad/1391639841_911785.html; Peru: http://elcomercio.pe/mundo/latinoamerica/ecuador-bonil-rectifica-caricatura-que-molesto-correa-noticia-1707442


for political purposes. 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, despite articles detailing Ecuador’s acquisition of large “Heron” drones from Israel Aerospace Industries. In January 2014, however, President Correa revealed Ecuador’s first domestically manufactured drone. The “unmanned aerial vehicle,” known as UAV-2 Gavilan, or Hawk, was created by the Ecuadorian Air force as a surveillance tool for areas that are difficult to access, such as the Amazon rainforest. While the president announced that the drones, which can transmit photo and video footage in real time, will be used primarily in the fight against drug trafficking, given that there appears to be little oversight or regulation of the domestic UAV program, some have voiced concerns that the drones could be used to track and gather information on the political opposition.

Journalists and bloggers have often been subject to threats and harassment online. In May 2013, Martin Pallares, a journalist for the newspaper El Comercio, was subject to harassment and death threats on Twitter, where he was warned that he would be murdered if he remained in Ecuador. In December 2013, Juan Carlos Calderon, an investigative journalist and the founder of Plan V, a digital magazine about corruption, received multiple threats, which he largely ignored until two “menacing-looking” men came to his house looking for him.

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. In April 2014, after a column she wrote criticizing President Correa’s U.S. trip appeared in El Universo, journalist and active Twitter user Betty Escobar, a long-time target of President Correa’s anti-press broadcasts, received a frightening threat at her home in New York. Flowers were left at her door along with a message forewarning that her “friends in Ecuador” would be paying her a visit. Her parents and aunt, who live in Ecuador, received similar threats the same day. Ms. Escobar filed complaints with the New York City Police Department and the District Attorney in Guayas, Ecuador. Although the case is still under investigation, it is noteworthy as it is the first report of a journalist living overseas being threatened for an article that appeared in an Ecuadorian newspaper. Finally, in May 2014, Marlon Puertas, an editor and writer,
Ecuador was threatened on Twitter, when a hashtag implying that he ought to be shot gained traction. The account responsible for the campaign has since been deactivated.\(^{72}\)

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. The websites of independent human rights organizations have been targeted on occasion, and have been subject to distributed denial-of-service (DDoS) attacks and unexplained disruptions. Although the sites’ administrators suspect government involvement, no party has taken responsibility.

In late 2013 and early 2014, government websites as well as the personal email and Twitter accounts of government officials were subject to cyberattacks from groups such as Anonymous. The accounts of prominent political figures such as Ecuador’s ambassador to the United States and the president of the national assembly were allegedly targeted. Important civic dates, such as the August 10\(^{th}\) commemoration of the Battle of Independence, also tend to cause a spike in cyberattacks, often against the government. On August 10, 2013, the websites of many small Ecuadorian towns were disabled, and multiple government websites were defaced.\(^{73}\) In March 2014, the president’s Twitter account was hacked by Anonymous. The hacktivist group used President Correa’s account 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.\(^{74}\)


\(^{73}\) The press release with the video posted by Anonymous can be seen here: http://www.elcomercio.com/politica/sitio-ConsejoParticipacionCiudadana-hackeado-Ecuador_0_971903008.html

Egypt

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>15</td>
<td>15</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>33</td>
<td>33</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>60</td>
<td>60</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

**Population**: 84.7 million

**Internet Penetration 2013**: 50 percent

**Social Media/ICT Apps Blocked**: No

**Political/Social Content Blocked**: No

**Bloggers/ICT Users Arrested**: Yes

**Press Freedom 2014 Status**: Not Free

---

**Key Developments: May 2013 – May 2014**

- Authorities repeatedly suspended telecommunications service in the Sinai Peninsula during military operations, disrupting the flow of information to and from the territory (see **Obstacles to Access**).

- The country’s highly divisive political environment has resulted in increasing verbal harassment between social media users and a declining willingness to speak out on contentious issues, resulting in self-censorship (see **Limits on Content**).

- In a referendum, Egyptians passed a new constitution that “guarantees” freedom of expression in theory, while outlining punishments for broadly defined offenses that could apply to online speech and preserving military trials for civilians (see **Violations of User Rights**).

- An increasing number of reporters and staff at online news agencies were detained over the past year, particularly while covering antigovernment protests. Prison sentences ranged from suspended sentences to several years. Popular bloggers and political activists continued to face trumped up charges, often for attending unlicensed protests (see **Violations of User Rights**).
Introduction

On June 30, 2013, a record number of Egyptians took to the streets to signal their discontent with the country’s Islamist trajectory and to demand early presidential elections. The protest was spearheaded by an apparent grassroots movement called Tamarod ("rebel"). As a result, Defense Minister and Commander in Chief of the Egyptian Armed Forces Abdel Fattah el-Sisi issued an ultimatum to the country’s “political forces” to “address the demands of the Egyptian people” within 48 hours. But President Mohamed Morsi, elected one year earlier as the candidate from the Muslim Brotherhood’s Freedom and Justice Party, refused to back down and broadcasted his defiance on television and social media. On July 3, 2013, he was detained by the military and replaced by the head of the Constitutional Court, Adly Mansour. A government was then formed out of a loose coalition of anti-Brotherhood and civilian figures.

The ensuing crisis led to deep fissures within Egyptian society. The stalemate between supporters of the military takeover and the ousted president was broken when security forces violently stormed two large sit-ins of Morsi supporters at dawn on August 14, 2013, leaving more than 800 dead.1 After the issuing of a transitional roadmap, the banning of the Muslim Brotherhood as a terrorist organization, and the passage of a new constitution, el-Sisi resigned from his post as minister of defense and declared his candidacy for new presidential elections. He was subsequently declared the winner on June 3, 2014, officially obtaining over 96 percent of the vote.

Since then, polarization and paranoia has led to the prosecution of activists, and the banning of organizations such as the April 6th Movement, a respected left-leaning activist and political group that had been highly critical of both the military and the Brotherhood. Numerous journalists and staff at news sites linked to independent outlets, to the Brotherhood, and to April 6th, have been assaulted and arrested for covering antigovernment protests or leaking government documents. Independent journalists have been beaten, detained, and even shot. A law outlawing protest, passed in November 2013, punishes protesters with seven-year prison terms; several people were imprisoned under the law. As a consequence, much of the political debate has quieted on the streets, but remains lively online. The Muslim Brotherhood maintains an online presence, although the arrest and imprisonment of most of its leaders means that it is primarily managed by those abroad. Well-known bloggers and activists, including many who were fundamental to the downfall of Hosni Mubarak, have faced trumped up charges as the military-led government seeks to limit all forms of dissent.

From 1993, when the internet was first introduced, until 2008, authorities showed a relaxed attitude toward internet use and did not censor websites or use high-end technologies to monitor discussions. However, with the rise of online campaigns to expose government fraud, document acts of police brutality, and call for large-scale protests, the government began to change its stance. Between 2008 and 2011, state police admitted to engaging in surveillance, online censorship, and cyberattacks—especially against sites related to the Muslim Brotherhood and other opposition movements.2

---


Generally speaking, dissent and objections to the military-backed rule have been dealt with harshly, both by the authorities and by progovernment mobs—organized or spontaneous—who took to beating opposition protesters, often under the approving eye of the police. In the most egregious case, journalist Mayada Ashraf was shot dead on March 28, 2014 while covering a protest; her last article had appeared online only hours earlier.³

**Obstacles to 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.⁴ Since then, ICT use has increased rapidly, with internet penetration growing from 16 percent in 2007 to 49.84 percent in April 2014. Mobile internet users via mobile phones or USB modems accounted for roughly 45.26 percent of all internet use, with ADSL use at around 36 percent. Egypt's mobile phone penetration rate was 119.89 percent in April 2014, amounting to 101.93 million mobile subscriptions.⁵

Although these figures are promising, there are a number of obstacles hindering access to ICTs, including an adult literacy rate of only 72 percent,⁶ poor telecommunications infrastructure in rural areas and urban slums, and flagging economic conditions. Moreover, ICTs and online culture are often viewed with suspicion and women's access to technology has become a growing concern after the revolution.⁷ In some cases, marginal religious figures have issued ‘fatwas’ against women using the internet without the presence of a male chaperone.⁸

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), whereas in Morocco, for instance, a 4 Mbps connection costs US$12.⁹ Prices are even lower in Gulf countries. 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, telephone lines are not universal, with large segments of the country not connected 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. To this can be added

---


the overall poverty of households, and it becomes clear that the vast majority of Egyptians do not have access to broadband internet. In an index that compares ICT prices to gross national income (GNI) per capita, Egypt ranks 77th out of 161 countries.

A user-led campaign was launched in December 2013, named “The Internet Revolution” (Thawrat al-Internet), to protest high prices, the “fair use policy”, and bad customer service on the part of providers. With innovative campaigns such as encouraging users to change to a 512 kbps connection for a month in order to financially pressure providers, or pay their bills in coins of EGP 1 and 0.5, the campaign succeeded in eliciting some response from the National Telecommunication Regulatory Authority (NTRA), who organized meetings with the ISPs to improve the quality of service. Nevertheless, the campaign continues.

Recent investment in telecommunications infrastructure has been limited since the revolution. The country’s economic crisis halted plans for a fourth mobile operator license and many foreign investment projects have ceased due to the increase in violence and political instability. Electricity blackouts due to fuel shortages also disrupted internet access in major cities. Blackouts, which reach their peak during the summer months, were a key mobilization point against President Morsi in 2013, and could be of political significance in the summer of 2014.

The Egyptian mobile phone market is divided between three companies. Mobinil, founded by construction magnate Naguib Sawiris, is now majority-owned by the French company Orange and had over 33 million subscribers by mid-2014. Vodafone Egypt, around 55 percent of which is owned by Vodafone, had over 41 million subscribers. Finally, Etisalat Misr is a subsidiary of Etisalat (UAE), which owns 66 percent of it, and had over 23 million subscribers. The state-owned company, Telecom Egypt, has a monopoly on landlines and, in April, obtained a license for a new mobile telephone company.

By the end of May 2014, Egypt had 44.5 million internet connections, with the market dominated by state-owned Telecom Egypt (under the name TE-Data). The Egyptian government has centralized internet infrastructure and fiber-optic cables into highly controllable “chokepoints.” In addition, virtually all of Egypt’s telecommunications infrastructure is owned by Telecom Egypt. Egypt’s five main ISPs lease lines from Telecom Egypt and resell bandwidth to over 200 smaller ISPs. 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, authorities disabled the country’s Border Gateway Protocol Routes, shutting down all internet traffic in less than one hour. Telecommunications companies were then ordered to cut mobile internet and text-messaging service under the terms of strict agreements they had signed with regulators. At the time, state

---

14 Erica Chenoweth, “Backfire in the Arab Spring,” Middle East Institute, September 1, 2011, http://www.mei.edu/content/backfire-arab-spring
intelligence agencies claimed that “foreign intelligence [was] using communication technologies to plan terrorist actions.”

In the second half of 2013, as the state engaged in widespread military operations in the Sinai peninsula in the pursuit of armed militant groups, it regularly shut down telephone and internet communications for several hours at a time in a bid to limit coordination between the militants, as well as to prevent the detonation of cellphone-triggered IEDs, a favored tactic of the militants. The military effort intensified in September 2013, during a massive campaign which saw the army combing entire villages and using heavy equipment. During the hours of the campaign, the entire peninsula was “cut off entirely from the outside world”. This was done with no warning to the residents who endured those repeated cuts.

Mobile service providers and ISPs are regulated by the NTRA and governed by the 2003 Telecommunication Regulation Law. The NTRAs 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. Officially, the NTRA is responsible for regulating the telecommunications industry 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**

No political, religious, or social websites were blocked in Egypt over the past year. Nonetheless, self-censorship has increased as a result of the polarized political climate. State-owned news outlets are unlikely to challenge crucial government decisions, while ordinary social media users risk harassment or, in some cases, professional repercussions for voicing their opinions on political topics. Despite these challenges, new, independent outlets are attempting to fill the gap, and Egyptians remain adept at utilizing social media as an instrument for positive change. The past coverage period saw a number of examples, particularly on issues of women’s rights.

---

Social networking tools and blog-hosting services are freely available, with government institutions also taking to them, primarily Facebook and to a lesser extent Twitter, to disseminate statements and news. Voice over Internet Protocol (VoIP) services are also widely used, 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.”

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. The debate over VoIP flared up again 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, citing that “pre-paid applications will face losses.” At the same time, political and security motives cannot be discounted, as the fact that Viber was originally developed by an Israeli company was regularly 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.

Egypt’s courts have made a number of high-profile rulings to block online content, with pornography a constant highlight of the rhetoric surrounding the state’s censorship campaign. A lawsuit launched in May 2013 accused the president of “ignoring the issue,” and claimed that a ban on pornography would cost only EGP 7 to 8 million (US$ 980,000 to 1.1 million). Egypt’s prosecutor-general had previously ordered government ministries to implement a 2009 ruling by the Supreme Administrative Court banning pornographic websites in late 2012. The decree was never formally implemented, with the ban estimated to cost as much as EGP 100 million (US$ 14 million), with significant effects to internet speeds. Civil society organizations have objected to the threat of a ban, both on grounds of freedom of expression but also because the expense would be too great. On August 24, 2013 the Administrative Court rejected the lawsuit. Nevertheless, several ISPs have implemented the court’s decision on a voluntarily basis, offering a “safe internet service” to subscribers.

While the courts have yet to force the blocking or deletion of these sites, progovernment users have taken up more informal tactics to force the deletion of social media accounts or groups that express views to which they are opposed. A Facebook campaign invited its supporters to report pro-Muslim Brotherhood pages en masse, ostensibly for violating the social network’s terms of use relating to

---

27 “NTRA: Viber, WhatsApp, BBM are free and cannot be priced,” Al Masry al Youm.
the incitement of violence. A government supporter, often introduced in television interviews as a ‘technology expert’, repeatedly stated that a Facebook page can easily be closed if 20 different accounts report it to the company.

Self-censorship has resurfaced to levels reminiscent of the pre-2011 days. The proliferation of cases against journalists on trumped up charges of ‘spreading false news’ and ‘aiding the enemy’—that is, the Muslim Brotherhood—has had a chilling effect on freedom of expression and reporting, with many choosing to stifle their own opinions out of concern for their own employment security or personal safety. Columnists and television presenters who were highly critical of the Supreme Council of the Armed Forces (SCAF) and then of former president Mohamed Morsi were placed in a precarious position in the post-June 2013 environment. A hostile military-led regime, backed by a public that seemed equally hostile to dissent, made any criticism of the military’s actions during the crackdown on the Muslim Brotherhood deeply unpopular.

This climate of intimidation, added to the intense political polarization, has altered the online news landscape. As most Muslim Brotherhood news websites maintain a nominal presence and are managed from abroad, the range of opinions has shrunk considerably, as has the professionalism of web outlets. In turn, state-owned media has espoused an extreme pro-military position, doing away with the modicum of diverse opinions once displayed. In such a climate of self-censorship and populism, in which many journalists are eager to reflect government positions, there has been less of a need to employ official state censorship. Once-leading opposition outlets, such as Al-Masry Al-Youm, promptly aligned with the state narrative, further limiting the diversity of opinions available to the public. This has contributed to an environment in which editors-in-chief and website administrators have opted to go along with populist sentiment rather than carry opposition voices.

However, some independent media sources have stepped up to fill the gap. One such example is Yanair (“January”), an online news portal in Arabic established by young professional journalists. While Yanair lacks a viable business model and relies primarily on opinion pieces rather than reporting, their opposition stance has rapidly earned them a large readership and a solid roster of opinion contributors. Another is Mada Masr, an English-language publication founded by former Egypt Independent journalists and contributors. Operating on a limited budget, Mada Masr has nevertheless succeeded in launching an Arabic portal alongside the English one, and its journalists have carried on the mission of providing objective and original reporting on current events. It has also distinguished itself with its primers and background articles, as well as hard-hitting cartoons.

Furthermore, there is very limited coverage of regional news both in traditional and online media. One of the few examples comes from Mandara, a news website focusing on the Sa‘eed, Egypt’s rural
and largely impoverished South. Mandara also offers training to budding journalists who report from the southern governorates. Coverage of the Sinai Peninsula, whose local population is caught in violence between armed forces and Islamist groups, is sparse. With little news reported in formal media, people turn to local activists and journalists who report on local events. Their coverage makes national news very sporadically.

In contrast to the online media landscape, the continued development of Egyptian social media reflects both users’ engagement in debate, as well as their selection of social media as a primary source of news. With 16.2 million subscribers in Egypt by the end of 2013, Facebook was the most visited website in the country. Egyptians account for around a quarter of all of the region’s Facebook users and the numbers continue to increase; over 2.6 million new Egyptian accounts were registered in the first half of 2014 alone.

Social media remains an arena for rhetorical sparring between supporters of the military-led government, backers of the deposed Muslim Brotherhood-dominated government, and the dwindling “revolutionary” movement, now a minority. In fact, after General Sisi issued an ultimatum to the Muslim Brotherhood-backed president, it was on Twitter that Morsi posted his rejection of the ultimatum.

The height of the social media war came in the aftermath of August 14, 2013, when security forces stormed two Muslim Brotherhood-supporting long-standing sit-ins in the squares of al-Nahda and Raba’a al-Adaweya, the latter significantly larger. The death toll of the operation was estimated by the Egyptian government to be 638 victims, while a Human Rights Watch report released on the first anniversary of the events put the death toll at “a minimum of 817 people and more likely at least 1,000.”

A four-fingered salute, usually drawn in black on a yellow background, emerged as a symbol of solidarity with the victims of the killings and, more broadly, with the ousted president. The symbol was de facto criminalized, leading to a number of harsh punishments against anyone who displayed it, including a protester who received a 2.5-year jail sentence for wearing a Raba’a pin, a child who was arrested for carrying a ruler with the symbol on it, and professional athletes

---

38 Massaad Abu Fajr is one such example, see www.facebook.com/massaad.abufajr; Federation of Journalists and reporters in Sinai, see www.facebook.com/fjr.sinai.
43 “Morsi Ousted While Sparring With Egyptian Army on Social Media,” Mashable, July 3, 2014, mashable.com/2013/07/03/egypt-social-media/.
46 “State-appointed body finds no evidence of rape at women’s prison,” Al Ahram Online, July 9, 2014, english.ahram.org.eg/NewsContent/1/64/105853/Egypt/Politics-/Stateappointed-body-finds-no-evidence-of-rape-at-w.aspx.
disciplined for performing the salute or wearing branded t-shirts. Online, many used the symbol as their avatars and profile pictures, both within and outside Egypt. Unsurprisingly, the symbol spawned a large number of parodies, mocking either the four-fingered salute or the cause behind it.

To circumvent the public hostility towards it, the Brotherhood has attempted to multiply its online presence by using other front organizations such as the “National Alliance to Support Legitimacy and Reject the Coup,” “Egyptians against the Coup,” and other smaller groups. The Muslim Brotherhood also launched a website for International Women’s Day on March 8, 2014, focusing on violations against female members and supporters of the Brotherhood.

After Field Marshall el-Sisi announced his intention to run for president on March 26, 2014, many independent activists, Muslim Brotherhood supporters, and other detractors of el-Sisi took to Twitter and Facebook to insult him with the Arabic hashtag translating to “Vote for the pimp.” In contrast, supporters of the Field Marshall used the hashtag “I will elect Sisi” to express support for his candidacy. Statistics about the anti-Sisi hashtag were widely shared by its supporters as proof of the general dislike of el-Sisi, overloading the Twitter analytics website Keyhole on March 29.

Speaking to the media, a renowned blogger stated that the hashtags came about because Twitter is "the only arena where [Sisi critics] can express their opposition.”

In May 2014, during the course of the short-lived presidential campaign which pitted Sisi against veteran politician Hamdeen Sabbahi, with Sisi and his supporters dominating the airwaves, Sabbahi’s supporters also took to social media. Debates with sparring hashtags based on the slogans of the candidates were commonplace, but faded with the end of the elections.

Rights groups and campaigns have also found a home on social media. Groups like “The Egyptian Movement for Change” (Kefaya), the 6th of April Movement, and “We Can See You” (Shayfenkom) have been successful in rallying for political causes through the use of social-networking sites. The “No Military Trials for Civilians” campaign is a primary example of sharing information and messages online, in order to rally supporters on the internet to participate in offline actions.

Women’s rights groups have emerged as key users of social media for advocacy. Campaigns such

---

51 See https://www.facebook.com/AllianceSupportingLegitimacy.
52 See http://sewomen.org.
as HarassMap and Baheya ya Masr have expertly used the internet to raise awareness, advocate for their positions, and rally supporters. Even primarily offline campaigns, such as the “feminist graffiti” NooNeswa or the theatre and storytelling of the BuSSy collectives have made excellent use of social media to spread the word about their activities.57

Violations of User Rights

Political events over the past year have threatened the safety of Egypt’s digital activists, online journalists, and ordinary social media users. Within hours of the ousting of Mohamed Morsi, the army closed down several Islamist television channels and arrested five journalists from Al Jazeera Mubasher Misr.58 The crackdown extended to online media, with reporters and editors from Muslim Brotherhood-linked sites such as Rassd and IkhanWeb arrested and imprisoned. However, arrests and assaults have not been limited to Islamist-leaning media outlets. Independent journalists, particularly those investigating military operations or covering antigovernment protests, have been targeted with beatings and even live ammunition, resulting in the death of reporter Mayada Ashraf. In an environment where two of the main organized opposition movements—the Muslim Brotherhood and the April 6th Movement—have been banned, the post-Morsi, military-led regime has demonstrated its intent to close down avenues for dissent.

The removal of Mohamed Morsi by the army in July 2013 led to a suspension of the existing constitution, which had been signed into law by Morsi in December 2012. In its place, the constitution of 1971, as amended in 2011, took effect until the subsequent passing of a new constitution in January 2014 under the provisional government of Acting President Adly Mansour and Defense Minister Abdel Fattah el Sisi. The latter has been the public face of post-Morsi Egypt and, as such, has been the recipient of much of the praise and criticism for Egypt’s current state of affairs. Criticism of the government’s crackdown on all opposition forces in the country has thus resulted in an increase in military prosecutions under the charge of “insulting the army.” Online activity is adjudicated under two judicial systems: civilian courts under laws derivative of the Mubarak era,59 and military courts operating under broad powers with little accountability.

The new constitution came into effect on January 18, 2014,60 after a campaigning process fraught with irregularities and a vote boycotted by the opposition.61 It 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

57 The campaigns mentioned can be accessed at harassmap.org, fb.me/BaheyaYaMasr, fb.me/WomenGraffiti, and fb.me/TheBuSSyProject.
60 All articles of the constitution mentioned here are based from the English translation developed by International IDEA and available at www.atlanticcouncil.org/images/publications/20131206EgyptConstitution_Dec.pdf.
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.” Article 211 outlines the establishment of a “National Media Council” tasked with regulating “the affairs 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, examined 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. Most of those trials occur outside of the capital and away from the public eye.

In late 2013, the Ministry of Interior announced a draft antiterrorism bill amending the penal code and the criminal procedures law. The proposed legislation classifies a larger number of crimes as terrorism and provides for the establishment of a “Terrorism Prosecutor’s Office” which would likely be subject to fewer checks and appeal provisions than normal courts. The draft threatens internet freedom, as it would allow the police to monitor internet traffic and social media activity to “prevent their use for terrorist purposes.”

Furthermore, Article 27 of the draft 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.” Further, 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. After heavy backlash from the international

62 The full text reads, “It is prohibited to censor, confiscate, suspend or shut down Egyptian newspapers and media outlets in any way. Exception may be made for limited censorship in times of war or general mobilization. No custodial sanction shall be imposed for crimes committed by way of publication or the public nature thereof. Punishments for crimes connected with incitement to violence or discrimination amongst citizens, or impugning the honor of individuals are specified by law.” See “Egypt’s constitution 2013 vs. 2012: A comparison” Al Ahram Online, December 12, 2013, http://english.ahram.org.eg/NewsContent/1/0/88644/Egypt/0/Egypts-constitution-2013-vs-2012-A-comparison.aspx.
63 “Egypt panel approves ‘conditional military trials of civilians’,” Ahram Online, November 21, 2013, english.ahram.org.eg/NewsContent/1/64/87113/Egypt/Politics-/Egypt-panel-approves-conditional-military-trials-o.aspx.
66 “Egypt’s Anti-Terrorism Law to Target Internet,” Global Voices.
In a shift from the previous coverage period, this year witnessed an increase in the number of arrests and prosecutions of online journalists, particularly those affiliated with the Muslim Brotherhood or its Freedom and Justice Party (FJP). According to the Committee to Protect Journalists, Abdel Rahman Shaheen and Ahmed al-Ajos, two reporters with the news website Freedom and Justice News Gate, were arrested on April 9, 2014 for “inciting and committing violence.” Shaheen was sentenced to three years by a court in Suez. Al-Ajos was released on bail in September and his trial was set for October.

Three individuals from the opposition news website Rassd were arrested. Executive Director Samhi Mustafa and co-founder Abdullah al-Fakharany were taken into custody in August 2013, initially for “disturbing the peace” and other charges unrelated to their profession. However, the charges were later switched to “spreading chaos” and “spreading false information” as part of their coverage of the armed incursion into the Raba’a protests. Separately, Rassd correspondent Mahmoud Abdel Nabi was charged with possessing weapons and inciting a riot while covering protests and clashes between pro-Morsi and pro-army supporters in Alexandria in July 2013.

Many journalists continue to be subjected to military trials. Amr al-Qazzaz and Islam Farahat, two Rassd journalists, were arrested in November 2013 and accused of leaking videos of el-Sisi, as well as government documents. While al-Qazzaz was acquitted, Farahat was sentenced to one year in prison and a fine of EGP 500 (US$ 70).

Khaled Hamza, a political advisor in the Muslim Brotherhood and former editor-in-chief of its website, Ikhwanweb, was arrested with four others while attempting to cross the border into Sudan in February 2014. All were handed one-year prison sentences by a military court.

Two journalists from the pro-Morsi online news network Yaqeen were arrested in late December 2013 while covering student protests at Al Azhar University, which turned violent.


Ahmed Gamal and journalist Saaid Shihata were held for months without charge until April 2014, when they were accused of “participating in an illegal demonstration and assaulting a police officer.” Gamal, who has not been formally charged, reportedly went on hunger strike on August 25.76 Shihata was set to be tried in May 2014.

Independent journalists have also been arrested during the coverage period of this year. Muhamed Sabry, a blogger, freelance journalist, and photographer, was handed a six-month suspended sentence on November 3, 2013.77 He was charged under a military court with “entering a prohibited military zone and filming a military facility” while investigating the killing of Egyptian soldiers near the Rafah border crossing.78

Numerous journalists have been arrested on charges of joining illegal protests while covering demonstrations as part of their professional assignments. Ahmed Fouad, a journalist at the news website Karmoz, was also arrested while covering antigovernment demonstrations on January 25, 2014, the third anniversary of the 2011 revolution. He was accused of numerous crimes unrelated to his journalistic work, including “joining a group that aims to disrupt the law,” “blocking a road,” “possessing a weapon,” and “demonstrating without permission.” Karim Shalaby, a reporter for Al-Masdar news site linked to the April 6th Movement, was also arrested on January 25.79 Similarly, Hussein Hassan Sobhy, a reporter for the news site Radio Horytna, was arrested while covering a pro-Brotherhood protest in February 2014.80 He was not released on bail until September 17.81

On October 5, 2013, award-winning journalist Ahmed Abu-Deraa was sentenced to six months in prison, a sentence that was later suspended. Abu-Deraa, the 2012 recipient of the European Union’s Samir Kassir award for freedom of the press, was charged with “intentionally spreading false information about the military.”82 The investigative journalist had given details of injuries and the destruction of six homes and part of a mosque in the village of Sheikh Zawad during a military operation to create a buffer zone with Gaza.83 News sources speculated over whether he was arrested for several articles,84 which appeared online, or a related Facebook post.85

On February 15, 2014, police arrested the administrator of a Muslim Brotherhood-affiliated Facebook page, charging him with “spreading false news, inciting violence against security forces” as well as

77 For Sabry’s Twitter profile, see https://twitter.com/muhamedsabry.
79 The movement was banned on April 28, 2014.
“spreading personal information of security officers.” The 25-year old, only identified by his initials, is believed to still be in prison pending trial.

Authorities have made extensive use of the restrictive protest law to arrest several of Egypt's high-profile political activists, who use social media to interact with followers, document human rights violations, and mobilize protests. In many cases, their online activities have been key to building their following and, conversely, in bringing unwanted attention from police and security forces. One of these revolutionary activists is blogger Alaa Abdel-Fattah, who has suffered legal harassment from the governments of Hosni Mubarak, the SCAF, Mohammed Morsi, and the post-Morsi military-led regime. Abdel-Fattah is a founding member of the anti-Brotherhood and antimilitary Revolutionary Front.

In the latest case, Abdel-Fattah was arrested along with two dozen co-defendants at a November 2013 demonstration organized by the "No Military Trials for Civilians" campaign, of which his sister is a founder. He was charged with assaulting a police officer and taking part in an illegal protest. Although he had announced his intention to voluntarily present himself to the authorities upon hearing the accusation, police raided his house at dawn and violently beat him and his wife while arresting him, also confiscating electronic devices from his house. Abdel Fattah was subsequently detained in prison for nearly four months before being released on bail of EGP 10,000 (US$1,500). On June 11, physically prohibited from entering the courtroom, he was sentenced in absentia along with 24 others to 15 years in jail for assaulting a police officer and taking part in an illegal protest. The defendants were also fined EGP 100,000 (US$ 14,000) each and placed under five years of police surveillance. However, only Abdel-Fattah and renowned activists Wael Metwally and Mohamed Abdel-Rahman ("Noubi") were imprisoned after the sentence was read. The trio had been part of a wider group of activists and prisoners who had started a hunger strike against Egypt's new protest law. Due to Egyptian law on sentences handed out in absentia, they were granted a retrial in August 2014. One month later, they were released on bail as the court's judge stepped down from the case.

Abdel-Fattah was once again arrested in October 2014. On June 1, 2013, Coptic lawyer Romani Murad Saad was sentenced in absentia to one year in prison and a fine of 500 EGP (US$80) for allegedly insulting Islam. He was also made to pay EGP 10,000

(US$1,500) in civil damages to the plaintiffs. The lawsuit stems from a heated online argument that took place two years ago in a Facebook group related to young lawyers in the Egyptians city of Assiut. Saad and Islamist lawyers argued over the 2012 presidential elections, which pitted Islamist Mohamed Morsi against former regime insider Ahmed Shafik. Unhappy with his political opinions, the Islamist lawyers later alleged that Murad had insulted Islam during a private discussion at a library. Although subsequent evidence was never provided to prove the allegations, the trial went ahead and Saad was sentenced in absentia.

In May 2014, 19-year-old Kirollos Shawky Atallah, a Christian, was detained after he posted a picture of the Muslim prophet Mohammed on his Facebook page along with an insulting comment, causing riots in his village in the governorate of Luxor. Villagers pelted his house with bricks. One month later, on June 24, Atallah was sentenced to six years in prison on charges of “insulting Islam” and “inciting sectarian violence.” His attackers were released the next day.95

On January 23, 2014, Twitter and YouTube user Ahmed Anwar was found guilty of “insulting the Ministry of Interior, misusing the Internet, and harassment” in relation to a video he uploaded to YouTube. He was sentenced to three months in jail but was able to commute his sentence after paying EGP 10,000 (US$ 1,500).96 The video, uploaded in early 2012, featured mock commentary over footage of a public event of the ministry honoring singers and actors for “raising the morale of policemen.” Legal Affairs Director of the Gharbeya Security Directorate, part of the Ministry of the Interior, filed a complaint shortly after the video was posted, and an arrest warrant was issued in March 2013. Egyptian human rights organizations described the accusation as “yet another piece of evidence of the Egyptian authorities’ hostility and violations against internet users, in a desperate attempt to silence its critics.”97

Aside from arrests and prosecutions, online journalists have also been assaulted and arbitrarily detained, particularly while covering protests. Freelance photojournalist Mahmoud Abou Zeid “Shawkan” was beaten and detained during the August 2013 protests and, as of June 2014, remained in custody without charge.98 American journalist Mike Giglio, formerly of the Daily Beast and now at BuzzFeed, was also detained and beaten. He was released the same day.99 Giglio reported that the police confiscated his laptop and slapped him until he gave up his login password.

Journalists have also come under live fire while documenting protests.100 Mayada Ashraf, reporter for Al-Dustour and news site Masr al-Arabiyya, was shot dead on March 28, 2014 while covering

antigovernment demonstrations. The news outlet has been critical of the Brotherhood and the FJP. Her last article, which covered the protest, was published online that day.

Ordinary social media users have also been reprimanded by their employers for their social media posts. On February 16, 2014, Cairo University teaching assistant Ahmed Abdel Basset Mohamed was suspended from work for “insulting the university teaching staff” on his personal Facebook page. The teacher, who also posted the decision on Facebook, said that it was punitive action for “rejecting the murder of students inside the university campus.”

Restrictions on anonymity and the use of encryption software make it easier for these activists to be monitored and singled out by the authorities. Under Article 64 of the 2003 Telecommunications Law, the use of encryption devices is prohibited without the written consent of the NTRA, the military, and national security authorities. In addition, cybercafe customers must provide their names, email addresses, and mobile numbers to receive a personal identification number (PIN) to access the internet. Further, the Telecommunications Law allows the offices of the Presidency, Security, Intelligence, and the Administrative Control Authority to obtain citizens’ online information without prior consent in cases that concern national security.

Online surveillance by security agencies is a grave concern in Egypt. 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. RCS, produced by the Milan-based company “Hacking Team,” 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. Egypt-based endpoints for the reception of data channeled by RCS were identified by the researchers as recently as end of October 2013, indicating it was operational under the current militarily-led regime. 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.

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 such things 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 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 was reported listing 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.

Regarding cooperation between state security structures and the private sector, ISPs and mobile operators are obliged to maintain a database of their customers and to allow the government to access their databases. After the ending of a grace period issued by the MCIT, customers who do not have their National ID numbers registered with their phone companies will have their phone lines cut. The NTRA has suggested that it would suspend additional phone numbers for mobile operators who fail to abide by the new rules. 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.

Egyptian government websites have faced cyberattacks, with reports of overseas hackers targeting the sites for political reasons. In July 2013, Turkish collective Ayyıldız Tim took responsibility for defacing a number of Egyptian government websites, including that of the Ministry of Military Production, in support of Mohamed Morsi. Egyptian hackers have also been responsible...
for attacks overseas, such defacements of a series of government websites in the United Arab Emirates,\textsuperscript{117} supposed to be in retaliation of Emirati support for the ousting of Morsi.\textsuperscript{118}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\end{flushleft}
Estonia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>3</td>
<td>3</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>9</td>
<td>8</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 1.3 million

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Penetration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Media/ICT Apps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Political/Social</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bloggers/ICT Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Press Freedom Status</td>
<td></td>
<td>Free</td>
</tr>
</tbody>
</table>

Key Developments: May 2013 – May 2014

- Estonia continues to be one of the most wired countries in the world, with increasing internet access and online participation among citizens (see Obstacles to Access).
- In October 2013, 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 Limits on Content).
- Estonia continues to improve its cybersecurity programs, strengthening its capacity to prevent and combat cyberattacks (see Violations of User Rights).
Introduction

Estonia ranks among 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 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.

The first internet connections in the country were introduced in 1992 at academic facilities in Tallinn and Tartu. The national telecommunication monopoly was subsequently privatized with the inclusion of Finnish and Swedish telecommunication companies, and a fiber-optic backbone was built with modern fixed and mobile communications services. 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. Children’s safety on the internet is a high priority, and the special program “Targalt Internetis” (Wiser Internet) is dedicated to country-wide training and awareness-building activities on internet safety issues for parents and children. In addition, a 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

On October 10, 2013, 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 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 would 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

---

Obstacles to 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 80 percent in 2013, compared to about 78 percent in 2012 and 71 percent in 2008.4 There were also over 2 million mobile phone subscriptions, translating to a mobile phone penetration rate of 160 percent.5 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 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 80 percent in 2013, compared to about 78 percent in 2012 and 71 percent in 2008.4 There were also over 2 million mobile phone subscriptions, translating to a mobile phone penetration rate of 160 percent.5 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.6 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 2013, 4G services covered over 95 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.7 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.

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.8 Today, there are over 200 operators offering such services, including six mobile phone companies 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.9

In 2009, the Estonian Internet Foundation was established to manage Estonia’s top level domain,

---

“.ee.” 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 and management capabilities, 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).

Limits on Content

Restrictions on internet content and communications in Estonia are among the lightest in the world. YouTube, Facebook, Twitter, LinkedIn and many other international video-sharing and social-networking sites are widely available and popular. Moreover, 32 percent of Estonians use the internet for uploading and sharing original content such as photographs, music, and text—the highest level of shared public communication in Europe. Nevertheless, due in part to Estonia’s strong privacy laws, there are some instances of content removal. Most of these cases involve civil court orders to remove inappropriate or off-topic reader comments from online news sites. Comments are similarly 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 self-censorship and 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. 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 issued the final ruling on the case, upholding 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.

In another case regarding intermediary liability, the European Court of Justice issued a ruling on May 13, 2014, stating that the 1995 Data Protection Directive applied to the activities of search engines.

---

11 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.
like Google, and that these companies may have to remove search results if the data is deemed to violate an individual’s right to privacy. Cases in which search engines may have to remove links are limited only to searches for an individual’s name; the original content in the link would not be removed and would still appear in other searches, but the link would no longer appear in search results for the individual who requested the removal. Many critics of this ruling argue 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.

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.16 The list of blocked sites is transparent and is available to the public.

Over the past few years, the removal of online content related to possible copyright infringement on YouTube and other video streaming services has increased, resulting in the removal of over 80,000 videos. This process was greatly facilitated by requests from copyright enforcement organizations representing Estonian authors.17 Hundreds of videos have been removed from YouTube for copyright violations even though some of the videos were posted by the authors themselves who were apparently not aware of the activities of copyright enforcement organizations representing their rights.18 All of these requests came from individuals or companies; the Estonian government has not issued any requests for removal of content on any of Google’s platforms, including YouTube, since at least 2010.19

There are over 70,000 active Estonian-language blogs on the internet, including an increasing number of group, project, and corporate blogs. The vibrancy and activities of the blogosphere are frequently covered by traditional media, particularly when blog discussions center on civic issues. The fact that so many Estonians are both computer literate and connected to the internet has created unique opportunities for the Estonian government. In addition to hosting virtual trade fairs and an online embassy, the Estonian president’s office has its own Twitter and Facebook accounts, and releases messages on its YouTube channel.20

Estonia has the largest functioning public-key infrastructure21 in Europe, based on the use of

21 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.
electronic certificates maintained on the national identification (ID) card. 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 authentication and digital signature purposes. The Digital Signature Act, adopted in 2000, 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. 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.

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.

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 supervision of the processing of personal data, management of databases and access to public information." The current version of the PDPA came into force in 2008.

Estonia is currently in the process of amending the Penal Code to comply with the European Council Framework Decision 2008/913/JHA of 28 November 2008 on "combating certain forms and expressions of racism and xenophobia by means of criminal law" in order to establish a framework

---

23 Ibid., accessed July 15, 2013.
on hate speech criminalization in the country. 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. This process is still ongoing and has become the topic of significant public debate within the country.

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 such 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, 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 the report of the Estonian Parliament Security Authorities Surveillance Select Committee that oversees the practices of surveillance agencies and security agencies, there were over 7,400 cases of requests for information based on court orders in 2012, an increase of 9 percent from the previous year. The select committee has been established to exercise supervision over the legality of surveillance and the activities of the Security Police. The committee monitors the conformity of the activities of the Security Police Board with the constitution, the Surveillance Act, and other regulations on security agencies.

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 involved parents in increasing the protection of children on the internet.  

Awareness of the importance of ICT security in both private and business use has increased significantly since the cyberattacks that occurred 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, increasing competence in cyber security, improving the legal framework, bolstering international cooperation, and raising 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 over the past few years as defense exercises that have served to improve the technical resilience of Estonia’s telecommunication networks and other critical infrastructure.

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.

---

38 Ibid.
Ethiopia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Free</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td></td>
<td></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>29</td>
<td>29</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>79</td>
<td>80</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 89.2 million
Internet Penetration 2013: 2 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Telecom services worsened, characterized by frequently dropped phone calls, prolonged internet service interruptions, and slow response times to service failures (see Obstacles to Access).
- Facebook, Twitter, Yahoo, and CNN were inaccessible for 12 hours in July 2013, while the number of permanently blocked webpages also increased (see Limits on Content).
- A law enacted in November 2013 gives the Information Network Security Agency (INSA) carte blanche to inspect private online activities without oversight (see Violations of User Rights).
- The government launched sophisticated surveillance malware against several online journalists in the Ethiopian diaspora and dissidents in exile (see Violations of User Rights).
- Six bloggers of the prominent Zone9 blogging collective were arrested in April 2014 on charges of terrorism (see Violations of User Rights).
Ethiopia

Introduction

Ethiopia continues to have one of the lowest rates of internet and mobile phone connectivity in the world, as meager infrastructure, government monopoly over the telecommunications sector, and obstructive telecom policies have significantly hindered the growth of information and communication technologies (ICTs) in the country. Coupled with highly repressive laws and tactics aimed at restricting freedom of expression and access to information, internet freedom in Ethiopia is consistently rated the worst in sub-Saharan Africa and among the worst in the world.

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. 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 mostly in the diaspora. Surveillance of mobile phone and internet networks is systematic and widespread, enabled by Chinese-made technology that allows for the interception of SMS text messages, recording of phone calls, and centralized monitoring of online activities. The government also employs commentators and trolls to proactively manipulate the online news and information landscape.

During the report’s coverage period, internet freedom in Ethiopia worsened due to increasing restrictions on access to social media and communications tools, such as Storify, and the temporary blocking of Facebook and Twitter in July 2013. A new law passed in November 2013 gave the Information Network Security Agency (INSA) carte blanche to track private online communications and investigate electronic devices without oversight. In addition, a number of diaspora journalists and exiled dissidents were targeted with surveillance malware, demonstrating a growing level of sophistication in the government’s effort to silence critical voices that extends beyond the country’s borders.

In 2014, the Ethiopian authorities increased their crackdown against bloggers and online journalists, using the country’s harsh laws to prosecute individuals for their online activities and quash dissent. Most alarmingly, six bloggers from the critical Zone9 blogging collective and three journalists associated with Zone9 were arrested in late April 2014 on charges of terrorism, which, under the Telecom Fraud Offenses Law and anti-terrorism proclamation, can entail a sentence of up to 20 years in prison if the bloggers are found guilty. The Zone9 case was repeatedly stalled by the courts throughout 2014, leaving the bloggers in pre-trial detention for over six months as of late-2014. Meanwhile, two online radio journalists were arrested and detained for a week without charges in August 2013, and the prominent dissident blogger, Eskinder Nega, and award-winning journalist, Reeyot Alemu, continue to serve lengthy prison sentences, despite international pressure for their release. The overall crackdown has had a major chilling effect on internet freedom and freedom of expression in the country, leading to increasing levels of self-censorship among online journalists, bloggers, and ordinary users alike.

Obstacles to Access

In 2013 and 2014, access to ICTs in Ethiopia remained extremely limited, hampered by slow speeds and the state’s tight grip on the telecom sector.² According to the International Telecommunications Union (ITU), internet penetration stood at a mere 1.9 percent in 2013, up from 1.5 percent in 2012.³ Only 0.25 percent of the population had access to fixed-broadband internet, increasing from 0.01 percent in 2012.⁴ Ethiopians had more access to mobile phone services, with mobile phone penetration rates increasing from 22 percent in 2012 to 27 percent in 2013,⁵ though such access rates still lag behind a regional average of 80 percent.⁶ Meanwhile, less than 5 percent of the population has a mobile-broadband subscription.⁷ Radio remains the principal mass medium through which most Ethiopians stay informed.

While access to the internet via mobile phones increased slightly in the last year, prohibitively expensive mobile data packages still posed a significant financial obstacle for the majority of the population in Ethiopia, where per capita income in 2013 stood at US$470.⁸ Ethiopia’s telecom market is very unsaturated due to monopolistic control, providing customers with few options at arbitrary prices.⁹ Prices are set by the state-controlled Ethio Telecom and kept artificially high. As of mid-2014, monthly packages cost between ETB 200 and 3,000 (US$10 to $150) for 1 to 30 GB of 3G mobile services.¹⁰

The computer remains the most practical option for going online, though in 2014, personal computers are still prohibitively expensive. The combined cost of purchasing a computer, initiating an internet connection, and paying usage charges makes internet access beyond the reach of most Ethiopians. Consequently, only 2 percent of Ethiopian households had internet access in their homes in 2013.¹¹ The majority of internet users rely on cybercafes to log online, leading to a growth of cybercafes in recent years, particularly in large cities. 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. For years, logging into an email account and opening a single message could take as long as

---

⁴ International Telecommunication Union, “Fixed (Wired)-Broadband Subscriptions, 2000-2013.”
⁵ International Telecommunication Union, “Mobile-Cellular Telephone Subscriptions, 2000-2013.”
six minutes at a standard cybercafe with broadband in the capital city.\textsuperscript{12} According to May 2014 data from Akamai’s “State of the Internet” report, Ethiopia has an average connection speed of 1.2 Mbps (compared to a global average of 3.9 Mbps).\textsuperscript{13} Meanwhile, Ethiopia’s broadband adoption (characterized by connection speeds greater than 4 Mbps) is less than 3 percent,\textsuperscript{14} while the country’s narrowband adoption (connection speed below 256 Kbps) is about 20 percent among those with access.\textsuperscript{15} Numerous users reported that internet and text messaging speeds were extremely slow during the coverage period, with services completely unavailable at times.\textsuperscript{16} Frequent electricity outages are also a contributing factor to poor telecom services.

Despite reports of massive investments from Chinese telecom companies in recent years,\textsuperscript{17} 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. The country 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. In an effort to expand connectivity, the government has reportedly installed several thousand kilometers of fiber-optic cable throughout the country over the past few years.\textsuperscript{18} Construction of the East African Submarine Cable System (EASSy) was completed and launched in July 2010, but its effects on Ethiopia have yet to be seen as of mid-2014.\textsuperscript{19}

The space for independent initiatives in the ICT sector, entrepreneurial or otherwise, is extremely limited,\textsuperscript{20} with state-owned Ethio Telecom holding a firm monopoly over internet and mobile phone services in the country. Consequently, all connections to the international internet are completely centralized via Ethio Telecom, 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.\textsuperscript{21} During the coverage period, one Renesys report found that 40 percent of Ethiopia’s networks were down for a few hours on July 18, 2013 as a result of a disruption on the SEACOM network, though the exact reason for the disruption was unknown.\textsuperscript{22} In September 2013, a number of cybercafe owners in Ethiopia reported an increasing trend of unpredictable internet connections and speeds beginning in June that result-


\textsuperscript{22} Renesys, Twitter post, July 18, 2013, 5:10pm, https://twitter.com/renesys/status/357955490237513729/photo/1.
ed in a significant decline in business, with internet connections reported as unavailable for up to 15 days in a month.\footnote{Bewket Abebe, “Internet Connection Grief,” Addis Fortune, September 29, 2013.}

Mobile phone networks---also completely centralized under Ethio Telecom---are similarly vulnerable to service disruptions and shutdowns by the government, which often occur during politically sensitive times. During the coverage period, there were frequent reports of dropped cell phone and landline calls, complete network blackouts in many parts of the country,\footnote{Yonas Abiye, “Network Blackout Hits Addis As Parliament Slams Ethio Telecom,” The Reporter, February 8, 2014, http://allafrica.com/stories/201402102129.html.} and overlapping voices in calls. The latter phenomenon led people to suspect government engagement in a widespread eavesdropping scheme (see “Violations of User Rights” for details on surveillance).


have led to increasing fears that the Chinese may also be assisting the authorities in developing more robust internet and mobile phone censorship and surveillance capacities.\textsuperscript{33}

The Ethiopian Broadcasting Authority (EBA) and the Ethiopian Telecommunications Agency (ETA) are the primary regulatory bodies overseeing the telecommunications sector. These two organizations were established as autonomous federal agencies, but both are highly controlled government bodies.

**Limits on Content**

During the coverage period, over a hundred websites remained inaccessible in Ethiopia, with a greater number of online tools and services targeted for blocking. A June 2014 report affirmed the government’s efforts to recruit and train progovernment citizens to attack politically objectionable content online.

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 Ethio Telecom-controlled international gateway. A more sophisticated strategy of blocking websites based on a keyword in the URL path, known as deep-packet inspection (DPI),\textsuperscript{34} was detected in May 2012 when the Tor network—an online tool that enables users to browse anonymously—was blocked.\textsuperscript{35}

In January 2014, an independent test conducted by a researcher based in the country found 120 unique URLs that were inaccessible in the country, 62 of which were Ethiopian news websites, 14 of which were political party websites, 37 of which were blogs, and 7 of which were television and online radio websites.\textsuperscript{36} During the test, some websites opened at the first attempt but were inaccessible when refreshed. The test also found that select tools and services on Google’s Android operating system on smart phones were inaccessible at irregular intervals but for unclear reasons. A separate test on over 1,400 URLs between July and August 2013 by the OpenNet Initiative in partnership with


\textsuperscript{36} Test conducted by an anonymous researcher contracted by Freedom House.
Human Rights Watch similarly found 62 websites blocked altogether and numerous others intermittently inaccessible.  

International news outlets were increasingly targeted for censorship. Al Arabiya, a Saudi Arabia-based media outlet, and both of Al Jazeera’s Arabic and English websites were intermittently blocked during the coverage period. In July 2013, websites belonging to Yahoo and CNN were reportedly inaccessible for about 12 hours. Facebook and Twitter were also targets of the short-term July 2013 blocking. There was no evident impetus or reason for the short-term blocking, and other major services such as Gmail and new outlets such as the New York Times remained accessible. Nevertheless, the incident further increased worries over reports of government plans to block popular social media tools completely. Facebook and Twitter platforms were otherwise generally accessible, although some individual Facebook groups belonging to opposition individuals remained blocked altogether, particularly when accessed via the unencrypted (http://) URL pathway. Meanwhile, the social media curation tool Storify—first blocked in July 2012—remained blocked during the coverage period, while the URL shortening tool Bit.ly was inexplicably blocked in late 2013.

In the past few years, the authorities have become more sophisticated in their censorship techniques, electing to block select webpages as opposed to entire websites. Critical online news articles are usually targeted, such as an August 2012 Forbes article titled, “Requiem for a Reprobate Ethiopian Tyrant Should Not Be Lionized,” which was blocked for criticizing the local and global praise of the former prime minister’s debatable economic growth achievements; the article remained blocked as of June 2014. A July 2013 YouTube video of the antigovernment Muslim protests that occurred from 2012-13 was also blocked as of late 2013.

International blog-hosting platforms such as Blogspot have been frequently blocked since the disputed parliamentary elections of 2005, during which the opposition used online communication tools to organize and disseminate information that was critical of the ruling Ethiopian People’s Revolutionary Democratic Front. In 2007, the government instituted a blanket block on the domain

---


38 “Ethiopia 2013 Testing Results,” Citizen Lab (Google Drive document), accessed September 8, 2014, https://docs.google.com/spreadsheet/pub?key=0Ah0XQ-1lDRPYdE9Yy8PNWZudEdXMX4VvK0TCJ1NKe&gid=0


40 An old Amharic saying that demonstrates the country’s deep-rooted culture of fear—“Stay away from electricity and politics”—recently evolved to: “Stay away from Social Media.” The contemporary saying implies that giving one’s political opinions via social media could cause grave bodily injury similar to exposing oneself to electricity.


44 Research conducted by Freedom House consultant.


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,\(^{47}\) as opposed to the entire blogging platform. Nazret, however, remained completely blocked as of June 2014. Circumvention strategies have also been targeted, with the term “proxy” yielding no search results on Google,\(^ {48}\) according to an independent source. Meanwhile, the terms “sex” or “porn” are still searchable.

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. Some restrictions are also placed on mobile phones, such as the requirement for a text message to obtain prior approval from Ethio Telecom if it is to be sent to more than ten recipients.\(^ {49}\) A bulk text message sent without prior approval is automatically blocked.

There are no procedures for determining which websites are blocked or why, which precludes 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), Ethio Telecom, and the ministry of ICT—seem to be implementing their own lists, contributing to a phenomenon of inconsistent blocking.

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. Local newspapers and web outlets receive their news and information from regime critics and opposition organizations in the diaspora. While the domestic Ethiopian blogosphere has been expanding, most blogging activity on Ethiopian issues still originates in the diaspora. Few Ethiopian journalists work for both the domestic print media and overseas online outlets due to the threat of repercussions.

Increasing repression against journalists and bloggers has had a major chilling effect on expression online, particularly following the arrest of the Zone9 bloggers in April 2014 (see “Violations of User Rights”). Fear of pervasive surveillance has led to widespread self-censorship, and many bloggers publish anonymously to avoid reprisals.\(^ {50}\) Notably, users on social media platforms such as Facebook and Twitter seem to practice a lower degree of self-censorship, which may be due to poor awareness of privacy settings, or the perception that posts on social media are anonymous or more secure.

---

47 Zone9 blog hosted at: [http://zone9ethio.blogspot.com/](http://zone9ethio.blogspot.com/).

48 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 2014, pg 56, 58.

49 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.

Despite extremely low levels of internet access, the authorities employ progovernment commentators and trolls to proactively manipulate the online news and information landscape. Acrimonious exchanges between commentators on apologist websites and an array of diaspora critics and opposition figures have become common in online political debates. There was a noticeable increase in the number of progovernment commentators during the coverage period, as confirmed in a 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 who report directly to government officials had been trained on how to post progovernment comments and criticize antigovernment articles on social media platforms. 51

As the country prepares for the upcoming 2015 National Election, the state media has stepped up its campaign against the press in general and the use of social media in particular, claiming that foreign agents and terrorists are using social media to destabilize the country. Consequently, many civil society groups based in the country are wary of mobilizing against the government, and calls for protest come mostly from the Ethiopian diaspora rather than from local activists who fear the government’s violent crackdowns against protest movements.

Nevertheless, over the past few years, Facebook has become one of the most popular mediums through which Ethiopians share and consume information. Social media services have also become significant platforms for political deliberation and social justice campaigns. For example, in September 2013, a group of young Ethiopian bloggers and activists based in Addis Ababa launched a Facebook and Twitter campaign on the occasion of Ethiopia’s New Year celebration to share their vision of a better Ethiopia, using the hashtag #EthiopianDream. 52 In November 2013, Ethiopians responded to the Saudi government’s crackdown on undocumented Ethiopian immigrants in Saudi Arabia by organizing the online campaign, #SomeoneTellSaudiArabia, to protest the abusive treatment of Ethiopian immigrants. 53

Netizen activism was particularly pronounced and widespread following the arrest of six Zone9 bloggers and three journalists for their alleged affiliation with the Zone9 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. Within five days, the #FreeZone9Bloggers hashtag had been tweeted more than 8,000 times. 54 Unfortunately, the international campaign elicited no response from the government, and the imprisoned bloggers and journalists are still awaiting trial on charges of terrorism as of late-2014.

---

Violations of User Rights

During the coverage period, the Ethiopian government’s already limited space for online expression continued to deteriorate alongside its poor treatment of journalists. A new proclamation passed in November 2013 empowered INSA with sweeping surveillance capabilities without judicial oversight. Sophisticated malware was launched against online radio journalists and dissidents in exile, while repression against bloggers and ICT users in the country increased notably. Six bloggers of the critical Zone9 blogging collective were arrested for their alleged terrorist activities.

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 also provides certain protections for media workers, such as prohibiting the pre-trial detention of journalists. Nevertheless, the press law also includes problematic provisions that contradict constitutional protections and restrict free expression. For example, media outlets are required to obtain licenses to operate through an onerous registration process that applies to all outlets, regardless of size, though it is uncertain whether the press law’s broad language encompasses online media. Penalties for violating the registration requirement and other restrictions on content, such as defamation, involve high fines and up to two and three years in prison, respectively.

In September 2012, the government codified specific restrictions on various telecommunications activities through the passage of the Telecom Fraud Offences law, which revised a 1996 law that had placed bans on certain communication applications, such as Voice over Internet Protocol (VoIP)—including Skype and Google Voice—call back services, and internet-based fax services. Under the new law, the penalties under the preexisting ban were toughened, increasing the fine and maximum prison sentence from five to eight years for offending 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 equipment—including smart phones—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.

60 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.
62 A Proclamation on Telecom Fraud Offence.
Most alarmingly, the Telecom Fraud Offences law extended the violations and penalties defined in the 2009 Anti-Terrorism Proclamation and 2004 Criminal Code to electronic communications, which are broadly defined yet 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, vaguely defined. Meanwhile, the criminal code holds any “author, originator or publisher” criminally liable for content allegedly linked to offenses such as treason, espionage, or incitement, which carries with it the penalty of up to life imprisonment or death. The criminal code also penalizes the publication of a “false rumor” with up to three years in prison.

In 2014, the Ethiopian authorities increased their crackdown against bloggers and online journalists, using the country’s harsh laws to prosecute individuals for their online activities and silence dissent. Most alarmingly, six bloggers from the critical Zone9 blogging collective and three journalists associated with Zone9 were arrested in late April 2014 on charges of terrorism. They were accused of “working with foreign organizations that claim to be human rights activists… and receiving finance to incite public violence through social media,” though the arrests had occurred just days following Zone9’s Facebook post announcing plans to resume its activism. The blogging collective had been inactive for seven months as a result of “a considerable amount of surveillance and harassment” the bloggers had suffered at the hands of security agents for their writings and social media activism. Despite widespread international condemnation of the Zone9 arrests, the detainees were denied bail in August and remained in jail as of fall 2014, awaiting trial. 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.

Numerous other journalists and media outlets—both online and print—were targeted for arrest and prosecutions during the coverage period, including Darsema Sori and Khalid Mohammed who were arrested in August 2013 for their work with the online radio station, Radio Bilal, which is known for its extensive coverage of the 2012-13 antigovernment protests organized by Ethiopian Muslims.

63 Article 19, “Ethiopia: Proclamation on Telecom Fraud Offences.”
They were released after being held for a week without charges, but the arrests were in keeping with the government’s concerted efforts to silence the protests.

Given the high degree of online repression in Ethiopia, some political commentators use proxy servers and anonymizing tools to hide their identities when publishing online and to circumvent filtering, though the ability to communicate anonymously has become more difficult. The Tor Network anonymizing tool was blocked in May 2012, confirming that the government has deployed deep-packet inspection technology, and Google searches of the term “proxy” mysteriously yield no results.

Anonymity is further compromised by strict SIM card registration requirements. Upon purchase of a SIM card through Ethio Telecom or an authorized reseller, individuals must provide their full name, address, government-issued identification number, and a passport-sized photograph. Ethio Telecom’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-2014.

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 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 Ethio Telecom network and has the ability to intercept emails and web chats.

Another ZTE technology, known as ZSmart, is a customer management database installed at Ethio Telecom 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.

In November 2013, a new Cyber Security Law expanded the surveillance powers of the Information Network Security Agency (INSA)—the government body established in 2011 to preside over the se-
security of the country’s critical communications infrastructure. According to reports, the law states that “social media outlets, blogs and other internet related media have great capabilities to instigate war, to damage the country’s image and create havoc in the economic atmosphere of the country”—setting the logic for expanding INSA’s duties to include developing offensive cyber capabilities and ICT tools. The proclamation also empowers INSA to investigate computers, networks, internet, radio, television, and social media platforms “for any possible damage to the country’s social, economic, political and psychological well being.”

INSA reportedly uses sophisticated spyware, such as 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 threats. A leaked document confirmed that the UK-based company, Gamma International, had provided Ethio Telecom with the FinFisher surveillance toolkit at some point between April and July 2012. In addition, research conducted by Citizen Lab in March 2013 worryingly found evidence of an Ethio Telecom-initiated FinSpy campaign launched against users that employed pictures of the exiled prodemocracy group, Ginbot 7, as bait.

There has been an increasing trend of exiled dissidents targeted with surveillance malware in the past few years. In April 2013, Tadesse Kersmo, a senior member of Ginbot-7 living in exile in the United Kingdom since 2009, came across the above-mentioned Citizen Lab FinSpy report and noticed that one of the spyware campaign’s bait was a picture of himself. He contacted Citizen Lab to have his computer examined and found that FinSpy had been active on his computer over two days in June 2012. The spyware may have transmitted any or all of Kersmo’s emails, chats, Skype calls, files, and web searches to a server based in Ethiopia, which could have provided the authorities with names of contacts, colleagues, and family members still living in the country. In February 2014, Privacy International filed a criminal complaint to the UK’s National Cyber Crime Unit on Kersmo’s behalf, urging them to investigate the potential unlawful interception of communications.

In the same month, the Electronic Frontier Foundation filed a similar suit in the United States on behalf of another Ethiopian dissident (and American citizen) identified publicly under the pseudonym

---

81 Marquis-Boire, “You Only Click Twice.”
Mr. Kidane. Kidane’s computer had also been found infected with the FinSpy malware sometime between late October 2012 and March 2013, which had secretly recorded dozens of his Skype calls, copied emails he had sent, and logged a web search conducted by his son on the history of sports medicine for a school research project. The FinSpy IP address was linked to a server belonging to Ethio Telecom.

Recent Citizen Lab research published in February 2014 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, VA. 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, and intercept Skype calls/chats. While Hacking Team claims that they do not deal with “repressive regimes,” the RCS virus sent via sophisticated bait to the two ESAT employees made it clear that the attack was targeted, and researchers have strong suspicions of the Ethiopian government’s involvement.

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. 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 monitor user activity themselves.

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. Bloggers from Zone9, for example, reported suffering a considerable amount of harassment for their work, leading them to go silent for several months. Shortly after the blog announced on Facebook that it was resuming activities in April 2014, six Zone9 bloggers were arrested and sent to a federal detention center in Addis Ababa where the torture of detainees is reportedly common. The active Gmail accounts belonging to sev-

eral of the Zone9 bloggers\textsuperscript{94} while in detention suggests that they may have been forced give their passwords to security officials against their will.

\textsuperscript{94} Anonymous Freedom House researcher reported seeing several of the detained Zone9 bloggers actively online in Gmail chat.
France

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</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>3</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>4</td>
<td>4</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>20</td>
<td>20</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 63.9 million

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Penetration 2013:</td>
<td>82%</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 2014 Status:</td>
<td>Free</td>
</tr>
</tbody>
</table>

Key Developments: May 2013 – May 2014

- Pressure on internet companies increased, with France responsible for 87 percent of all removal requests received by Twitter in the second half of 2013. Twitter was also ordered by a French court to help identify authors of racist and hateful tweets (see Limits on Content).

- French users no longer face the threat of having their internet access suspended for repeated copyright violations, due to a change in the controversial HADOPI laws. Users now face reduced fines (see Violations of User Rights).

- In a victory for free speech, a French woman accused of defamation by the Ministry of the Interior was found not guilty by a court in May 2014. Amal Bentounsi had appeared in an online video in which she decried impunity for police brutality (see Violations of User Rights).

- Concerns over electronic surveillance increased after the passage of legislation in December 2013 that extended surveillance powers of intelligences agencies while failing to require judicial approval for their activities (see Violations of User Rights).
Introduction

France has a highly developed telecommunications infrastructure and a history of innovation in information and communications technologies (ICTs). 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. 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. Hate speech, defamation, copyright, and privacy are highly contentious issues relevant to French cyberspace. On several occasions over the past years, politicians have proposed highly restrictive measures, such as the imprisonment of frequent visitors to extremist websites and the mandatory registration of online news editors. A bill was also drafted that would ban the online sale of goods below market prices, thereby hurting e-commerce in a bid to protect brick and mortar shops. A similar bill was passed in June 2014 that hinders online bookstores from offering free delivery on already discounted books.

Intermediaries, particularly internet companies, have come under increasing pressure from French authorities for practices related to privacy, data collection, and hate speech. Twitter, frequently called on to take strong measures against “offensive” tweets, was ordered in 2013 by a French court to help identify authors of racist tweets. French authorities were responsible for 87 percent of all removal requests received by Twitter in the second half of 2013. In the first half of 2014, France ranked behind only Turkey for the highest number of requests. Google was fined EUR 150,000 (US$ 200,000) by the National Commission on Information Technology and Freedoms (CNIL) for violating European data protection laws, as implemented in France. The company will appeal the verdict, and similar cases from other EU countries are in the works.

France

The greatest concern for internet freedom advocates in France is electronic surveillance of the public. Leaks and reports have provided evidence that French intelligence authorities conduct mass surveillance and cooperate with their British and American counterparts, Government Communication Headquarters and the National Security Agency. In December 2013, an article was added to an omnibus bill on the military budget that extended legal powers for authorities to gain access to or record telephone conversations, emails, internet activity, personal location data and other electronic communications. The legislation provides for no judicial oversight and allows electronic surveillance for a broad range of purposes, including “national security,” the protection of France’s “scientific and economical potential,” and prevention of “terrorism” or “criminality.”

In a positive development, the most controversial provision of the French antipiracy law, referred to as the “HADOPI law” after the agency tasked with its implementation, was abolished in July 2013 and replaced with fines of up to EUR 1,500 (US$ 2,000) for copyright offenders. The law had been criticized by civil society organizations and international bodies for its “three strikes” provision, which required internet service providers (ISPs) to disconnect users from the internet for a period of two to twelve months when found to repeatedly engage in piracy. HADOPI since released a report revealing that, from 2009 to mid-2014, the agency sent over 3 million notices to French users to cease accessing pirated content. Just over 10 percent went on commit further offenses, resulting in a second warning letter. Of those warned a second time, only 0.45 percent, or 1,502 subscribers, received a third notice. Only 116 cases went to court and ended with fines ranging from EUR 250 to 700 (US$ 310 to 870).

Obstacles to Access

Since 2009, 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.

France had an internet penetration rate of 81.92 percent at the end of 2013, up from 70.68 percent in 2008. Fixed broadband use increased during the same period, from 28.50 percent to 38.79

---

percent.\(^\text{16}\) Regionally, penetration ranges from 84.4 percent in the Paris area to 65 percent in the northwest of France.\(^\text{17}\) 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.\(^\text{18}\) Over 5 million households did not use the internet in 2014,\(^\text{19}\) either due to obstacles to access, or personal choice.\(^\text{20}\) As French statisticians do not record information related to race, there is no government data relating to internet use according to ethnicity.\(^\text{21}\) On a positive note, there is little or no gender gap when it comes to internet access.\(^\text{22}\)

The average monthly cost of broadband internet access in France is approximately EUR 30 (US$ 43), for both ADSL\(^\text{23}\) and fiber-optic connections.\(^\text{24}\) Considering the average monthly income is EUR 2,359 (US$ 3,279),\(^\text{25}\) this makes internet access fairly affordable for a large percentage of the population. Companies such as Free Telecom also offer cheap internet access and mobile contracts through bundled deals.

There were 63.24 million mobile contracts in use in France at the end of 2013, representing a penetration rate of 98.50 percent.\(^\text{26}\) Over 23 million people use their mobile devices to access the internet,\(^\text{27}\) mostly in addition to a household connection.\(^\text{28}\)

There are no significant hurdles to prevent diverse business entities from 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). France Telecom is the formerly state-owned company that has since been


privatized and renamed Orange.\textsuperscript{29} The government still directly owns 13.5 percent of shares in the company, with a further 13.5 percent owned by a sovereign wealth fund operated by the state.\textsuperscript{30} Another provider, Free, is a relative newcomer in the mobile market—its 3G license was awarded by the French regulatory authority in December 2009—and has quickly picked up market share 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 €17 billion (US$22.85 billion) offer from Numericable.\textsuperscript{31} In the meantime, Bouygues Telecom began a round of strategic downsizing after failing to sell its assets.\textsuperscript{32}

The internet backbone consists of several interconnected networks run by ISPs and shared through peering or transit agreements. As such, there is no central internet backbone and ISPs are not required to lease bandwidth from a monopoly holder. However, an accident at an exchange node operated by the company Telehouse in March 2014 generated minor service disruptions in the French internet and major panic on social networks.\textsuperscript{33}

The telecommunications industry in France is regulated by the Regulatory Authority for Electronic and Postal Communication (ARCEP),\textsuperscript{34} while competition is regulated by France's Competition Authority and, more broadly, by the European Commission (EC).\textsuperscript{35} 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.\textsuperscript{36} The EC has previously stepped in when the independence of national telecommunications regulators seemed under threat, notably in Romania, Latvia, Lithuania, and Slovenia.\textsuperscript{37} ARCEP remains an independent and impartial body and decisions made by the regulator are usually seen as fair.

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.

\begin{itemize}
\item[30] 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, \url{https://europeanequities.nyex.com/en/products/equities/FR0000133308-XPAR/company-information}.
\item[34] “Autorité de Régulation des Communications Électroniques et des Poste,” \url{http://www.arcep.fr/index.php?id=18&L=1}.
\item[35] “Autorité de la concurrence,” \url{http://www.autoritedelaconcurrence.fr/user/index.php}.
\end{itemize}
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**

Although France has a strong record of an open and accessible internet, over the past few years the country has come under some criticism from online activists and free speech advocates. Controversially, French authorities have stepped up efforts to block or remove online content that is found to violate copyright protections or infringe on privacy. The most ardent defenders of free speech have been loath to see any sort of administrative filtering in France, fearing that laws such as LCEN, LPM, LOPPSI 2, and HADOPI, may eventually lead to a spillover whereby controversial yet legal sites are censored by administrative agencies and without a court order (See “Violations on User Rights”). Furthermore, child pornography and other illegal websites are blocked. 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 have been requested to remove the content or face blocking.

French law recognizes “the right to be forgotten” (le droit à l’oubli), which has its roots in rehabilitated criminals who did not wish to see their past cases publicized, having already “paid their debt to society” through jail time. In France, individuals could already request that defamatory content related to them can be removed through a court order in line with Article 29 of the 1881 Law on Press Infractions—related to insult, defamation, or denigration—and the 2004 Law for Trust in the Digital Economy (LCEN), which holds hosting providers liable if they fail to cooperate with a court decision. Some obligations were taken away from hosts and placed on the rights owners in a July 2012 ruling, however.

---

45 Loi pour la Confiance dans l’Économie Numérique.
The controversial issue has been taken up by the European Commission in recent years,\(^{47}\) resulting in proposals that have been criticized by some as impossible to enforce or threatening to free speech.\(^{48}\) In June 2013, the advocate-general of the European Court of Justice, Niilo Jaaskinen, stated his opinion that the right to be forgotten did not exist under current European data and privacy laws.\(^{49}\) However, on May 13, 2014, the ECJ found that the 1995 Data Protection Directive did apply to the activities of search engines like Google, and that these companies may have to remove certain search results if the data is deemed to violate an individual’s right to privacy.\(^{50}\) 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.\(^{51}\)

Intermediaries are coming under increasing pressure to cooperate with French authorities against defamation, copyright, and hate speech. French authorities are highly active in pursuing the removal of content online. As an indication, Google’s Transparency Report noted that the total number of content removal requests it received from the French government from January to June 2013 increased by 81 percent, compared to the previous six-month period.\(^{52}\) In November 2013, the High Court of Paris ordered Google, Yahoo, and Microsoft to remove links to 16 video streaming websites from search engine results. The action stemmed from a 2011 case brought to the French court by five different associations representing different sectors of the film and television industry. French ISPs were also ordered to block access to the websites.\(^{53}\)

In a separate case from November 2013, a French court ordered Google to remove links to images of Max Mosley that were originally published by the British newspaper *News of the World*, which

---


53 Andy, “Court orders Google, Microsoft & Yahoo to make pirate sites disappear,” Torrek Freak, November 29, 2013, [http://torrentfreak.com/court-orders-google-microsoft-yahoo-to-make-pirate-sites-disappear-131129/](http://torrentfreak.com/court-orders-google-microsoft-yahoo-to-make-pirate-sites-disappear-131129/). The associations included the Film Makers Association (APC), National Federation of Film Distributors (FNDF), Union of Digital Video Editing (SEVN), the Union of Film Producers (UPF), and the Union of Independent Producers (SPI).
closed after a high-profile phone-hacking scandal. Mosley had sued the newspaper over the photos, which purported to show Mosley, formerly the president of the International Automobile Federation (FIA), at a Nazi-themed orgy with prostitutes.

In July 2013, Twitter complied with a court order filed six months earlier to reveal the identity of authors of hateful and anti-Semitic tweets to human rights associations. Twitter also gave a special account to SOS Homophobia, an LGBT rights NGO, allowing the charity to quickly and easily report homophobic tweets to Twitter staff. Indeed, in January 2013, the French Minister for Woman’s Rights and a government spokesperson, Najat Vallaud-Belkacem, had called for Twitter to take greater responsibility in preventing the posting of hate speech on the site. However, the proposal was criticized as a danger to free speech, potentially allowing the government to classify unfavorable opinions under the vague term of hate speech. The move would also place an unfair burden on intermediaries, forcing them to use their discretion to prescreen content that could be deemed as offensive. When it comes to the curtailing of illegal content, ISPs and mobile telephone companies who provide internet access currently have no obligation to preemptively review any of the content they transmit or store. Nevertheless, according to LCEN, they must take prompt action to withdraw the relevant content when informed of unlawful information or activity, or face the possibility of civil liability. Similarly, cybercafes and other public places which provide internet access have no responsibility to review the content which can be viewed by their customers but are liable in cases of illegal activities; as a result, cybercafes must log the activities of their customers (see “Violations of User Rights”).

In June 2013, a 2011 draft law that suggested new means by which various government agencies could force content owners to remove content or instruct ISPs to block webpages was finally rejected. The draft outlined procedures for blocking or removing online content under Article 18 of LCEN, “in case of violation, or where there is a serious risk of violation, of the maintenance of public order, the protection of minors, the protection of public health, the preservation of interests of the national defense, or the protection of physical persons.” However, the order came under fire from internet freedom activists and the e-commerce community, who pointed out that intermediaries could face an unfair responsibility to police content. There were also fears that, under the proposal’s vague wording, the law would be applicable to most websites rather than only those

France

engaged in e-commerce, as originally intended. This would have opened up the possibility that any website could be blocked arbitrarily and without due process under the proposal’s emergency clause.

The original passage of LCEN was met with criticism from many in France, including members of parliament (MPs) from the Socialist Party. The MPs submitted a brief to the Constitutional Court to review several clauses of LCEN that failed to define email as private correspondence (and thus subject to greater surveillance), “privatized justice” through administrative notices and extralegal take down procedures, and set a longer statute of limitations for online content versus traditional media. The grounds under which authorities could restrict access to communications were also criticized as overly broad and open to abuse.

French authorities are fairly transparent about what websites are blocked and why content must be taken down. Incitement of hatred, racism, Holocaust denial, child pornography, copyright infringement, and defamation are illegal. Requests to block or remove content can emanate from individuals, copyright holders, or government bodies. These requests must be reviewed by a court, which then instructs ISPs, content holders, or other intermediaries to implement its decision.

France is home to a highly diverse online media environment. In recent years, several French protests have been organized online, including demonstrations against cuts in government-supported programs such as education or changes to labor laws proposed in 2006. More recently, from January to April 2013, online campaigns such as those organized by the controversial figure Frigide Barjot and others mobilized large groups of demonstrators using social media networks to oppose legislation surrounding same-sex marriages. The legislation was passed in April 2013.

French digital rights and online freedom advocacy groups are very active and play a significant role in the country. For example, the group La Quadrature du Net successfully lobbied the European Parliament for an amendment to the EU Telecoms Package to ensure that no restrictions on internet access could be imposed without prior judicial approval. After the European Parliament rejected ACTA in July 2012, the group also published a proposal for a new regulatory framework on reforming copyright issues.

A petition on Change.org to stop Article 20 of the LPM received over 100,000 signatures. A Twitter
Violations of User Rights

France’s constitution guarantees freedom of speech, in accordance with the 1789 Declaration of the Rights of Man. 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.” 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. Laws such as LOPSSI 2, LCEN, LPM and the HADOPI 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 activities and have cooperated with their transatlantic counterparts in the United States and United Kingdom. Recently, efforts have been made to clarify the procedures behind such surveillance, although internet freedom advocates have pointed out that some of this legislation, such as that attached to the Law on Military Programming, falls short on checks and balances.

Major changes to the HADOPI laws on copyright were enacted by the government in May 2013, after the publication of the Lescure Report, a study commissioned by President François Hollande. The laws, HADOPI 1 and 2, take their name from France’s High Authority for the Distribution of Works and the Protection of Rights on the Internet, referred to by the French acronym HADOPI. The agency was introduced in 2009 in a bid to promote the distribution and protection of creative works on the internet. The most controversial aspect of its mandate was the graduated response mechanism, or “three-strikes” rule, which effectively cut off internet access to households that were found to have violated copyright laws after the issuance of two warnings. This punishment was largely denounced as a violation of the fundamental right of freedom of access to information on the internet. In July 2013, the government halted the practice of suspending broadband access, while reducing the set of fines incurred for copyright violations.

---


71 “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, 1789, accessed March 17, 2014, http://avalon.law.yale.edu/18th_century/rightsof.asp.


74 HADOPI 2 came after the constitutional court invalidated parts of HADOPI 1. Indeed, the first HADOPI was adopted in June 2009, but the constitutional court rejected two articles that were against the presumption of innocence. HADOPI 2 came in October 2009, improving the rejected articles and adding more details on the procedure.

75 Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet.


The copyright-enforcing agency has since attempted to encourage users to access content legally, as opposed to focusing on the punishment for illegal access. Indeed, at the end of 2013, HADOPI launched Offre Légale Hadopi (“Legal Offer”), a site listing over 300 websites that offer legal, copyright-friendly alternatives to illegal content. As a concept, it has been considered a great improvement on the PUR (“Promotion des Usages Responsables”) label of the past, which only classified approximately 30 suitable websites. Unfortunately, the site still lacks a search function, which would greatly improve its usability.78 HADOPI itself has had its budget slashed and, as an institution, may cease to exist as the French government is considering transferring it over to the Conseil Supérieur de l’Audiovisuel (CSA), the radio and television regulator.79

Online journalists, bloggers, and activists have been tried by the French authorities for offenses related to hacking, defamation, and hate speech. In some cases, they have been the victims of a lack of technical knowledge by the courts. For instance, in 2012, blogger and digital activist Olivier Laurelli (alias “Bloutouff”) was arrested for “illegally accessing” confidential documents related to the French Agency for Food, Environmental and Occupational Health and Safety (ANSES). The documents were not properly secured and were available through Google’s index.80 Laurelli, who runs his own VPN company, Toonux, published content from the documents on Reflets.info, the news community website he co-founded. The DCRI, a former intelligence agency linked to the Interior Minister, traced the actions back to the VPN and contacted Laurelli as its operator. He was acquitted of criminal charges by a lower court. However, in February 2014, he was found guilty of stealing and improperly retaining the documents, a charge carrying a EUR 3,000 (US$ 4,000) fine.

In a case that triggered defense from free speech advocates, Manuel Valls, the Minister of the Interior, sued Amal Bentounsi on charges of defamation against a public administration. Bentounsi, whose brother Amine was mistakenly killed by police in 2012, runs a site against police brutality and published a video in which she made a sarcastic comment about widespread impunity under the justice system.81 A court acquitted her of the charges in May 2014 in an important victory for free speech.82

Separately, at least one user was jailed for calling for violence online. In March 2014, the moderator of a Francophone jihadist site was sentenced to one year in jail, with two further years as a suspended sentence. Romain Letellier is reportedly the first to be convicted under a 2012 law against “cyber-jihadism” for broadcasting calls to violence on the website Ansar al-Haqq (Defenders of the Truth).83 He had also translated articles from Inspire, a magazine linked to al-Qaeda.

The Law on Guidelines and Programming for the Performance of Internal Security (LOPPSI 2), adopted in 2011, relates primarily to cybersecurity and the fight against child pornography. In the two years that it was debated, online activists highlighted concerns that by allowing administrative agencies to demand ISPs to filter content without a court order, the government would open the door to administrative filtering of other more legitimate sites without judicial approval. In July 2012, Fleur Pellerin, Minister for the Digital Economy, announced that Article 4 relating to the administrative filtering of child pornography would not be implemented without a court order. Article 23 grants the police with the authority to install malware—such as keyloggers and Trojan horses—on a suspect’s computer in the course of counterterrorism investigations, though authorization must come from a court order.

This law does not generally interfere with the right to anonymous communication for online users, although individuals are required to register their real names when purchasing new SIM cards or using cybercafes. In 2010, a law was briefly floated to require anyone who edits “a non-professional communication service online” to register their name, location, and phone number as part of a push to apply existing press regulations on to the blogosphere. However, numerous online advocates condemned the proposal in an online petition and the law was never enacted.

A number of concerns have been raised in the last year on the subject of electronic surveillance, particularly in light of revelations made by Edward Snowden on worldwide intelligence-gathering activities. While French officials and the French public initially expressed outrage at claims of mass surveillance of its citizens by America’s National Security Agency (NSA), subsequent leaks revealed that France has developed its own capabilities to tap into fiber-optic cables, allowing for the mass monitoring of internet and phone activities.

In June 2013, French daily newspaper Le Monde revealed the alleged existence of an extralegal surveillance program operated by the Directorate-General for External Security (DGSE), a French foreign intelligence agency. The DGSE maintains the capacity to intercept communications

84 Loi d’orientation et de programmation pour la performance de la sécurité intérieure.
91 “Germany, France and Spain ‘were all spying on citizens’,” Tom Whitehead, November 1, 2013, accessed March 17 2014, http://www.telegraph.co.uk/technology/10421835/Germany-France-and-Spain-were-all-spying-on-citizens.html.
between France and external countries in a plan that was ostensibly designed for counterterrorism purposes. In early July, additional reports surfaced from Le Monde indicating that metadata from telephone and computer activity—even within France—was systematically collected and stored at the DGSE facility in central Paris. This runs counter to existing French law, which only allows for counterterrorism agents within the Central Directorate of Interior Intelligence (DCRI) to request metadata related to a user’s telephone and internet activities. These limited requests must also be reviewed by the National Commission of Control for Security Interceptions (CNCIS), an independent administrative authority. In the case of the DGSE program, by contrast, seven different government agencies have access to this large body of user data without any legal basis or judicial oversight. Furthermore, the mandates and scope of operations of some of these agencies are also not strictly limited to counterterrorism.

Leaked documents have also revealed that French agencies cooperate with their foreign counterparts, including the NSA and the UK’s Government Communications Headquarters (GCHQ). The head of the NSA denied reports that the US monitored millions of phone calls and texts in France during the period of December 2012 to January 2013, instead saying that France’s own intelligence agencies carried out the collection of phone records and shared that data with the NSA. Indeed, Bernard Squarcini, head of the DCRI intelligence service until last year, said that he was surprised by the shocked reactions of French officials at the time, stating that this type of spying was standard practice for all countries, including France.

In early December 2013, new regulations on electronic surveillance were passed as part of a routine military spending bill (the Military Programming Law, or LPM). Critics fear that Article 20 of the LPM would significantly expand electronic surveillance of French residents and businesses, including the ability to gain access to or record phone conversations, emails, internet activity, personal location data, and other electronic communication data. The powers relate to the DCRI, three intelligence agencies under the Ministry of Defense, as well as anti-money laundering and customs agencies. The government argues that the law, which will not go into effect until 2015, is actually a new and

---

improved form of regulating surveillance powers that have been in place for years. However, the law does not provide a mechanism for judicial oversight and allows electronic surveillance for an overly-broad range of purposes, including "national security," the protection of France's "scientific and economical potential," and the prevention of "terrorism" or "criminality." Although officials claim that parliament, as well as the CNCIS, will oversee the spying, agencies have until 48 hours after monitoring has begun to seek approval from the CNCIS president and can continue their surveillance while awaiting his decision. Critics have pointed out that the CNCIS lacks the appropriate control mechanisms and independence from political interference, given that the CNCIS is composed of only three politicians.

Reporters Without Borders also lamented that Article 20 of the LPM was drafted with little input from local stakeholders, such as the National Digital Council (CNN) or the National Commission on Information Technology and Freedoms (CNIL). They pointed out that this "dereliction of the government's democratic obligations" came just days after the international community strengthened its commitment to stopping this kind of "snooping" in the form of a UN General Assembly resolution on "The right to privacy in the digital age," adopted on November 20, 2013.

Others are concerned that the bill is not only a danger to citizens' rights, but that it will also hurt business. Service providers fear that customers will increasingly doubt that their data is private and secure. Technology firms belonging to the Association of Internet Services Communities, including Google, Microsoft, Facebook, Skype and AOL, have criticized the scale of the proposed surveillance.

Although the LPM was passed by the Senate, a dissenting quorum of 60 deputies and senators can call on the Constitutional Council to examine the text's conformity with the constitution. To try to regain public faith, it has been suggested that the French government support a review of the bill by the court, as well as by the CNIL.

On April 30, 2014, a decree from the Interior Ministry replaced the DCRI with the newly-established General Directorate for Interior Security, known by its French acronym DGSI. Under its mandate,

---

the expanded agency engages in surveillance on French territory on matters related to national security or fundamental national interests.¹⁰¹

The French telecommunications company Orange was hit with two massive cyberattacks over the past year, occurring in February and May 2014. Hackers acquired the personal details of 800,000 and then 1.3 million customers, respectively. No financial details were reportedly gained.¹¹¹

¹⁰¹ According to Numerama.com, this includes matters related to foreign interference, terrorism, territorial integrity, radical groups, secrets related to national defense or the economic, industrial, or scientific potential of the country, international criminal organizations, and ICT crimes.

The Gambia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>N/A</td>
<td>19</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>n/a</td>
<td>21</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>n/a</td>
<td>25</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>N/A</td>
<td>65</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 1.9 million
Internet Penetration 2013: 14 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- In May 2013, the government began the process of liberalizing international gateway services (see Obstacles to Access).

- Internet cafe registration regulations were tightened in September 2013, requiring operators to provide thorough details for a license, as well as mandating the physical layout of cafes and the signs that must be displayed (see Obstacles to Access).

- Access to the internet was disconnected for 48 hours in March 2014. Shortly after, the popular voice over Internet Protocol (VoIP) platform Viber was blocked (see Obstacles to Access).

- Amendments to the 2009 Information Communication Act were passed in July 2013, criminalizing the use of the internet to criticize the president or spread false news with up to 15 years in prison (see Violation of User Rights).

- Prominent TV presenter Fatou Camara was arrested and accused of using the internet to defame the president in September 2013. She fled the country upon release on bail. Another individual was arrested in December for broadcasting an opposition political rally via Skype without a license (see Violation of User Rights).
Introduction

The Gambia first adopted the internet in 1998 through the United Nations Development Program’s Internet Initiative that helped establish the country’s infrastructural capacity to provide internet access. In more recent years, the Ministry of Communication Infrastructure and Information Technology has invested considerable attention to the development of information and communications technologies (ICTs) for the purposes of economic growth.

Nonetheless, 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 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. In 2014, at least 15 news and opposition websites were blocked, most of which are based abroad and operated by exiled Gambian journalists.

The government strengthened its ability to control the internet in 2013 and 2014 through both technical and legal means. In March 2014, internet access was disconnected for 48 hours, enabled by state control over the country’s telecommunications infrastructure, while the popular Voice over Internet Protocol (VoIP) application, Viber, was blocked a few weeks later. Internet cafe registration regulations were initiated in April 2013, requiring an onerous application process, and in September 2013, the regulator issued further guidelines that mandated specific requirements on the physical layout of cyber cafes and the signs that must be displayed.

Existing legal restrictions on freedom of expression were explicitly applied to the internet in July 2013 with the passage of amendments to the 2009 Information and Communications Act, which prescribed up to 15 years in prison, a fine of up to GMD 3 million (US$100,000), or both, for using the internet to criticize, impersonate, or spread “false news” about public officials. The law applies to Gambians both in the country and abroad.

These new amendments were also used in September 2013 to prosecute well-known TV journalist Fatou Camara (and former director of press and public relations for the office of the president), who was accused of spreading false news on the internet and defaming the president in an article published in the U.S.-based online outlet, Freedom Newspaper. Facing up to 15 years in prison if convicted, Camara fled to the United States upon release on bail. Another individual, Lasana Jobarteh, faced charges under the new internet law in December 2013 when he was arrested after an opposition political rally and accused of broadcasting the rally without a license. Jobarteh was using Skype on his iPad to transmit coverage of the rally to the Freedom Newspaper online outlet based abroad.

Technical attacks against opposition websites and critical news outlets are also common and widely believed to be perpetrated by the government. In June 2013, the email accounts belonging to the editors of U.S.-based American Street News (ASN) were hacked. While the government’s technical surveillance capabilities remain unknown, there is a pervasive belief that citizens’ communications are proactively filtered and monitored, legally enabled by the sweeping powers given to national

---

security agencies to intercept communications without judicial oversight under the 2009 Information
and Communications Act.

Obstacles to 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 14 percent in 2013, according to the latest data from the
International Telecommunication Union (ITU). Fixed-broadband subscriptions are still paltry,
however, at a penetration rate of a mere 0.02 percent in 2013, and internet infrastructure is virtually
nonexistent in rural areas, resulting in a significant urban-rural divide in access. By contrast, The
Gambia has one of the highest mobile phone penetrations in Africa, with an access rate of nearly
100 percent in 2013, up from 13 percent a decade ago, though only 1.2 percent of the population
has access to mobile broadband.

At a cost of about US$8 per month, fixed-line subscriptions are expensive for individual users in
The Gambia, where average monthly household incomes are less than US$50. 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 only for a small subset of the population who can
afford the unlimited 3G wireless packages that begin at about US$62 per month.

Meanwhile, connection speeds are very slow, averaging 1.2 Mbps (compared to a global average
of 3.9 Mbps), according to May 2014 data from Akamai’s “State of the Internet” report. In addition,
The Gambia’s broadband adoption rate (characterized by connection speeds greater than 4 Mbps)
was about 5 percent of the internet population, while the country’s narrowband adoption rate
(connection speed below 256 kbps) was 9 percent.

Rural areas suffer from poor cellular reception and network coverage, which is compounded by poor
infrastructure, frequent power cuts, and a lack of electricity. Moreover, network coverage of rural

ITU-D/Statistics/Pages/stat/default.aspx.
pdf.
tariff_profiles.htm.
com/stateoftheinternet/soti-visualizations.html#stoi-map.
9 Akamai, “Broadband Adoption (connections to Akamai >4 Mbps): The Gambia,” map visualization, The State of the Internet,
10 Akamai, “Narrowband Adoption (connections to Akamai <256 kbps): The Gambia,” map visualization, The State of the
11 Kebba Camara, “Electricity Blackout Within Kanifing Municipality Creates Outcry,” Foroyaa Newspaper, September 25, 2013,
areas has not been a priority for most service providers,\textsuperscript{12} making rural provinces in The Gambia one of the most “disconnected regions of the world.”\textsuperscript{13} Radio remains the principal mass medium through which most Gambians stay informed.

There are four internet service providers in The Gambia—Gamtel, QuantumNet, Netpage, and Airtip—that deliver service only in urban areas.\textsuperscript{14} Four GSM companies provide internet service for mobile devices: Africell and QCell, which are privately owned; the state-owned Gamtel’s subsidiary, Gamcel, which provides 3G internet services; and Comium, the newest private player in the market, which provides 2G internet services in addition to regular calls.\textsuperscript{15}

The Gambia Telecommunications Company Limited, Gamtel, owns the fiber-optic cable that runs across the country and is the sole fixed-line provider. As a state-owned entity, Gamtel also controls the international gateway, allowing private telecoms to lease the gateway for data services only. In May 2013, however, the government began the process of liberalizing international gateway services by granting international data transmission licenses to private telecom operators.\textsuperscript{16} Voice communications, on the other hand, remain purely state-owned and controlled as part of the government’s effort to protect Gamtel’s monopoly.

Meanwhile, the ACE (Africa Coast to Europe) submarine cable system landed in The Gambia in December 2012, connecting the country to the 14,000 kilometer fiber-optic cable that stretches from France down the west coast of Africa to South Africa.\textsuperscript{17} Controlled by Gamtel, the ACE cable was expected to boost bandwidth and drive new services at more affordable rates, but as of mid-2014, such improvements have yet to be realized.

Despite the recent liberalization of the international gateway, the Gambian government still exerts a significant level of control over internet access in the country. In April 2013, the regulator PURA issued a press release banning internet cafes from offering Voice over IP (VoIP) calling services such as Skype, citing the need to protect the country’s “national interest.”\textsuperscript{18} Cybercafes were also banned from offering internet dating services, providing no justification. In response to public outcry over the ban, the Ministry of Information and Communication Infrastructure issued another press release two days later, clarifying that the use of VoIP services was not in fact prohibited. Rather, the government restricted internet cafes from commercializing VoIP services, or charging additional rates for VoIP calls on top of standard internet access rates.\textsuperscript{19} People continued to use these services freely, especially on their personal devices.

\begin{itemize}
  \item\textsuperscript{12} Interviews by Freedom House, February 2014.
\end{itemize}
The Gambia

In March 2014, users within the country reported experiencing an internet blackout for 48 hours.\(^\text{20}\) Though the reason for the blackout remains unknown, observers suspected that the disruption was a result of the government’s efforts to block VoIP applications.\(^\text{21}\) The popular VoIP application, Viber, was subsequently blocked a week later.\(^\text{22}\) While the government denied involvement and hinted that the block may have been engineered by services providers,\(^\text{23}\) the government is said to believe that platforms such as Viber are enabling exiled Gambian journalists to deliver objectionable information to the public.\(^\text{24}\) Users reported that Viber was unblocked in July 2014 for unclear reasons.\(^\text{25}\) Meanwhile, the popular messaging application, WhatsApp, is unavailable for download in the country as of mid-2014, though users who have the application preinstalled are still able to use it.\(^\text{26}\)

The telecommunications sector is not well regulated, and like in many other sectors, businesses must contend with inefficient bureaucracies. 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 March 2013, it reportedly gifted two new cars to Gambian President Yahya Jammeh for his birthday, which subsequently led to a resumption of the QPOWER service in June.\(^\text{27}\)

Internet cafe operators must also contend with onerous and opaque regulatory obstacles. For example, 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.\(^\text{28}\) The registration requirement was initiated in April 2013, shortly after another directive was issued banning cybercafes from commercializing dating and VoIP services.\(^\text{29}\) Existing cybercafes were given the deadline of May 27, 2013 to submit their applications and registration fees to the regulatory agency or face closure.\(^\text{30}\)


\(^\text{23}\) 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.”


\(^\text{26}\) According to sources on the ground. Freedom House interview, April 2014.

\(^\text{27}\) Modou S. Joof, “QPOWER service is back,” Front Page International (blog), June 14, 2013, [http://frontpageinternational.wordpress.com/2013/06/14/qpower-service-is-back/#more-1127](http://frontpageinternational.wordpress.com/2013/06/14/qpower-service-is-back/#more-1127).


Later 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.31

The internet and other public utilities are 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.32 To some consumer activists, PURA has been an ineffective regulator that seems more concerned about its image than the interests of consumers.33 As it stands in 2014, PURA neither has the expertise, equipment, nor enforcement power to effectively carry out its mandate.34 Furthermore, PURA is not independent, at least in its composition. The president appoints the governing board of the regulatory body on the recommendation of the Minister of Finance and Economic Affairs.35

**Limits on Content**

During the coverage period, Voice over IP (VoIP) applications were targeted for blocking, along with numerous critical news outlets and opposition websites that are unavailable to Gambian citizens.

The Gambian government has been suspected of censoring the internet since at least 2006,36 with political websites targeted in particular. As of 2014, critical news outlets such as *Freedom Newspaper*, *The Gambia Echo*, *Hello Gambia*, *Jollof News*, and *Gainako* are blocked in the country, among a host of other news sites known for their criticism of the government.37 The blocked outlets are all based abroad and managed by exiled Gambian journalists, most of whom have been targets of the regime. At present, at least 15 webpages are blocked in the country overall, including webpages of activists based abroad.38

The popular VoIP platform, Viber, was blocked in March 201439 and unblocked in July 2014 for unclear reasons.40 The government denied involvement and hinted that it may have been engineered

---

33 Interviews by Freedom House, February 2014.
34 Interviews by Freedom House, January 2014.
38 Freedom House interviews, April 2014.
40 Freedom House interview, July 14, 2014.
The Gambia

by service providers, though the government is said to believe that platforms such as Viber are enabling exiled Gambian journalists to deliver objectionable information to the public. Otherwise, YouTube, Facebook, Twitter and international blog-hosting platforms were freely available.

There is no transparency behind the blocking of internet content in The Gambia, and efforts to access a blocked URL typically times out. While the government denies any involvement in the blocking of critical news websites, state control over the country’s single telecommunications provider, Gamtel, gives the authorities direct power to restrict access to any 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.

There have been no known reports of the government requiring content providers to remove content from the internet, preferring instead to block critical websites altogether. 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. Furthermore, pressure from the authorities in the form of arbitrary arrests, extralegal harassment, and blatant threats has led to a climate of fear and a severe degree of self-censorship among journalists, both online and offline. Independent online journalists are typically based abroad, while bloggers and online activists based in the country work anonymously.

Independent online media outlets also face the challenge of economic sustainability in a country where many businesses avoid advertising with critical outlets out of fear of government reprisals. Most critical news outlets are based abroad, operated by exiled dissidents and blocked within the country. Consequently, the online news and information landscape does not represent a diversity of political and social viewpoints. Nonetheless, there are small groups of locally based independent journalists and netizens who courageously push the boundaries of free expression and media freedom within The Gambia. One popular news blog, Front Page International (FPI)—managed and published by journalists based in country—is working to rally support for a more vibrant press.

While there is no concrete evidence that the authorities employ progovernment commentators to manipulate online content, observers assert that comments by trolls on many online forums distort the news and information landscape. Progovernment trolling activity tends to surge during times of political or social controversy. More often than not, online conversations between activists and regime apologists become abusive, resulting in quarrels and sometimes the use of hate speech.

41 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.”
Unfortunately, there have been no successful mass mobilization efforts through the use of ICTs for any particular issue in The Gambia. Sporadic efforts have been small and unsuccessful, mainly due to heavy-handed government repression against criticism and dissent.

Violations of User Rights

In July 2013, existing legal restrictions on freedom of expression were explicitly applied to the internet with the passage of amendments to the 2009 Information and Communications Act. A prominent TV presenter and an opposition supporter were arrested and charged with violations of the new internet restrictions. Technical attacks targeted the editors of an online news outlet based abroad.

The 1997 constitution categorically 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.”

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 criminalized defamation with a minimum prison sentence 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. The increased penalty is likely an effort to intimidate journalists and whistleblowers from seeking legal recourse for abuses at the hands of the authorities.

In July 2013, parliament passed amendments to the 2009 Information and Communication Act that specifically criminalizes online dissent, imposing prison sentences of up to 15 years, fines of up to GMD 3 million (about US$100,000), or both on individuals living in the Gambia or abroad found guilty of using the internet to criticize, impersonate, or spread “false news” about public officials. The government reportedly introduced the harsh internet law in response to online activism and the growing influence of critical news outlets, stemming primarily from abroad.

The new law was used in September 2013 to prosecute well-known TV journalist Fatou Camara (and former director of press and public relations for the office of the president), who was accused of spreading false news on the internet and defaming the president in an article published in the

U.S.-based online outlet, Freedom Newspaper.50 Before she was formally charged, Camara was held illegally for over three weeks without trial, during which she was reportedly forced to give intelligence officers her Facebook and email passwords.51 Concerned fans reported seeing her Facebook account active for unknown reasons while she was in detention.52 After Camara was granted bail of GMD 5 million (approximately US$153,000), she and the guarantors of her bail deposit were smuggled out of the country and now live in exile in the United States.53

In December 2013, opposition supporter Lasana Jobarteh was arrested at a political rally and accused of broadcasting the rally without a license.54 Jobarteh was using Skype on his iPad to transmit coverage of the rally to the Freedom Newspaper online outlet based abroad, which the authorities cursorily determined to be a violation of the broadcast license requirements under the 2009 Information and Communications Act.55 He was found guilty in July 2014 and sentenced to one year in prison or a fine of GMD 50,000 (about US$1,250), which he paid with support from members of his opposition party.56

The government places restrictions on anonymous communication through SIM card and local domain name registration requirements,57 the latter of which is managed by the regulatory authority.58 Meanwhile, the 2009 Information and Communications Act gives sweeping powers to national security agencies to “monitor, intercept and store communications” while also giving the regulator PURA the authority to “intrude communication for surveillance purposes,” all without judicial oversight.59 In addition, service providers are required to “implement the capability to allow authorized interception of communications.” Consequently, observers believe the government proactively monitors and intercepts citizens’ communications, particularly of activists and independent journalists whom the government perceives as a threat to national security.60 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.

60 Freedom House Interviews, February 2014.
The Gambia

The Gambia has one of the highest numbers of exiled journalists in the world, reflecting an environment extremely hostile to freedom of expression. Extralegal violence and intimidation against journalists are common, and the government routinely tries to prevent journalists from critical news outlets from covering certain events. Fortunately, there were no reports of online journalists or internet users targeted with violence or threats during the coverage period.

Technical attacks against opposition websites and critical news outlets are also common and widely believed to be perpetrated by the government. In June 2013, the email accounts belonging to the editors of U.S.-based American Street News (ASN) were hacked; the editors were reportedly informed by webmail host Yahoo that the hackers had redirected two days’ worth of all incoming emails to other accounts. Around the same time, there were two attempted hacking attacks against ASN’s website, which the online outlet’s IT staff was able to thwart. Further investigations traced the hacking efforts to a single IP address in The Gambia.

Georgia

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</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>8</td>
<td>8</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>11</td>
<td>11</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>26</td>
<td>26</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 4.5 million
Internet Penetration 2013: 43 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- New rules for the nomination of candidates to the Georgian National Communications Commission were implemented in October 2013, with the goal of improving the commission’s legitimacy and independence (see Obstacles to Access).

- Despite an increase in internet penetration, obstacles such as high prices for services, inadequate infrastructure, and low speed of internet remain, particularly for those in rural areas or with low incomes (see Obstacles to Access).

- In September 2013, a new online government portal was launched through which individuals can now make requests for public information (see Limits on Content).
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. In September 2013, a new online government portal was launched that allows citizens to access resources and request public information. However, not all government institutions have expressed a willingness to provide citizens with feedback; consequently, one-way interaction prevails on the online pages of these agencies.

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 the other commissioners of the GNCC, rather than directly by the president.

Despite a moderate internet penetration rate, in 2013, social media tools were used alongside traditional media outlets to document and respond to significant political and social events. The advent of diverse interactive maps and platforms enables users to report on matters of their concern.

Restrictions on online content in Georgia have decreased over past 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.

The appointment of a Consumers’ Rights Public Defender and creation of the Office of the Personal Data Protection Inspector in mid-2013 can be highlighted as a positive development for the protection of ICT users’ rights. If given sufficient power to operate and proven effective, independent, and autonomous in their functions, these new agencies may be able to effect tangible and substantial improvements to users’ rights in the near future.

Obstacles to Access

The number of internet and mobile 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. According to statistical data collected by the International Telecommunication Union (ITU), 43 percent of the population had access to the internet in 2013.
compared to 37 percent in 2012 and 10 percent in 2008. According to a countrywide survey conducted by the Caucasus Research Resource Centers (CRRC), 30 percent of the population accessed the internet on a daily basis in 2013, and the most active internet users are located in the capital. Only 5 percent of Georgians are unfamiliar with the internet altogether.

Internet service providers (ISPs) offer DSL broadband, fiber-optic, HSPA/EVDO, WiMAX and Wi-Fi connections. The average cost for an internet connection is US$20 per month, and the lowest price for a 5 Mbps DSL connection is about US$25 per month. There were about 580,000 fixed-line broadband internet connections in 2013, resulting in a fixed-broadband penetration rate of just over 9 percent, up from 0.6 percent in 2006.

Mobile phone penetration is greater than that of the internet and has continued to grow from 62 percent in 2008 to 115 percent in 2013. 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 cell 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). However, providers are offering new and somewhat less expensive services, including CDMA and EVDO technologies.

The Georgian National Communications Commission (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 between price plans. As of December 2013, 297,700 subscribers had made use of this service. According to a new national numbering plan, as of January 2012, all phone numbers have changed to align with international standards.

Despite expanding internet access, many users complain about the quality of connections and...
Georgia

suffer from frequent outages. For instance, according to the latest report of the Georgian National Communication Commission (GNCC), 77 written and 66 oral appeals were submitted by internet users, out of which 33 complained about the poor level of telecommunication service.\(^{18}\)

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 hours at a time, allowing them to access only Georgian websites during these disconnections, 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 2013-2014.

The web presence and internet usage of large companies and small businesses grew rapidly in 2013–2014, particularly as a result of social media tools and applications. Many established brands and companies such as banks, financial institutions, artists, public figures, and electronics stores have begun to use social media to promote their businesses and build customer support.\(^{19}\)

Cybercafes provide internet access at reasonable prices, but they are located mainly in large cities, and there are too few to meet the needs of the population. Most cafes have less than a dozen computers, and customers often have to wait as long as an hour for access. Internet cafes 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 utilise resources including Skype, bank services, telecommunication services, and electronic services developed by state (for example: property registration, e-auction, business registration, etc.).\(^{20}\) As of May 2014, 13 such centers are already operating in different regions and districts throughout the country.

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. Most ISPs are privately owned, and two ISPs control more than two-thirds of the market: SilkNet, with more than 46 percent share of the wired internet market, and Caucasus Online with a 32 percent share. Consequently, competition on the internet market is quite low. For example, 15 companies provide only 1 percent of the users in the capital with internet access.\(^{21}\) Three of the ISPs—Geocell, Magticom and Mobitel—are also mobile operators.\(^{22}\) The mobile internet

---


\(^{20}\) Find the information about the project: http://sda.gov.ge/ka-GE/p/ [in Georgian].


\(^{22}\) Data obtained in June 2014. For current data, see Top.ge at http://top.ge/all_report.php [in Georgian].
market is also dominated by two main providers, Magticom and Geocell. In 2013, Transparency International reported that many of the major telecommunications companies are owned by offshore shell companies.

The government of Georgia lacks a comprehensive strategy outlining a clear and long-term vision for developing the internet infrastructure throughout the country. To promote the strengthening of e-governance services in Georgia, the Data Exchange Agency of the Ministry of Justice of Georgia created an “e-Georgia” strategic document for the years of 2014-2018. 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. Additionally, 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.

The Georgian National Communications Commission (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. However, there is no significant difference between GNCC procedures for handling traditional media and those pertinent to telecommunications and internet issues; thus, 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 the GNCC, new rules for the nomination of candidates and the selection of the Head of Commission came into force on October 27, 2013. Consequently, the new chairman of the agency was elected by the commissioners themselves instead of the president of Georgia in May 2014.

Limits on Content

There is no evidence of online content being blocked in Georgia in 2013–2014. 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. 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.

---

23 As of 2013, Magticom possessed 42.8 percent of subscribers, which was followed by Geocell with 33.9 percent. The share of the third company, Mobitel accounted for 22.6 percent of this market.


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. In fact, content is so accessible that numerous sites offer illegal material such as pirated software, music, and movies, and the government has not enacted appropriate legal measures to combat the problem. ISPs still host websites with a great deal of pirated material, 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 and online resources 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 a lack of evenhanded decision-making. To date, however, such decisions regarding online content have been rare.

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. However, 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. An analysis of Facebook pages in 2013 and 2014 revealed that there

---

27 For example, the websites of Gol.ge (http://gol.ge/) and Adjarnet.com (http://adjaranet.com).
29 Focus group interview with more than 7 journalists and bloggers, November 25, 2013
30 Interview with the former civil servant. December 26, 2013.
31 Several blog-posts were published regarding such cases on the blog – “E-Participation in Georgia” – of Institute for Development of Freedom of Information: http://eparticipationge.wordpress.com/
are still fake accounts that solely post flattering comments of particular government officials. Specialists in Georgia claim that such forms of online manipulation indirectly restrict 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 apparent 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 1 percent of the total amount spent in the Georgian advertising market. At present, most online media outlets face difficulty in attracting advertisers. Less interest toward online advertisement from the private sector significantly stems from the relatively limited scope of the online audience.

Even though the Georgian blogosphere grew impressively to over 3,000 blogs in 2011, according to the latest available data, 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 two years, LGBT activists have started to extensively use online tools for coordination, distributing information, and protesting discrimination in the public sphere.

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, expenses, etc. 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 properly, and only a limited number of users utilize its services on a daily basis. According to representatives of Data Exchange Agency, currently My.gov.ge has about 8,000 registered users.

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, as a rule, attempt to respond to their questions in a comprehensive manner.

The majority of internet users (72 percent) 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). These figures mostly coincide with the data provided by the website ranking index Alexa.com, which indicates that Facebook is still the most frequently visited website in Georgia. It is worth noting that 24 percent of people considered the internet as their main source of information.

Different political and civil society groups post calls for action on Facebook and use social media platforms for communicating with their supporters. However, most forms of online activism to date have remained online and have not had a significant offline impact. Only a limited number of successful cases can be pinpointed, such as a group of guerrilla gardeners protesting against the building of a hotel in Vake Park who effectively used Facebook and Twitter to mobilize like-minded people; as a result of their consistent strategy, construction has been temporarily halted. Similarly, in order to make Georgia’s roads secure, the Partnership for Road Safety and Elva Community Engagement launched a website called “Friendly Roads,” enabling citizens to report and spot the most dangerous traffic infrastructure (the so-called “black spots”) in their neighborhood and commuting routes.

Another website, “Freedom to Internet,” was established by the Institute for Development of Freedom of Information together with Free Press Unlimited in June 2014. The website consists of an interactive map integrated onto the online platform that allows users, throughout the South Caucasus region and beyond, to report violations of internet users’ rights (including censorship, surveillance, violation of privacy, oppression due to online activity, and website filtering or blocking).

Violations of User Rights

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

40 Official web-site of Ministry of Internal Affairs of Georgia: http://videos.police.ge/?lang=en
44 National Democratic Institute, “Public Attitudes in Georgia: Results of an April 2014 Survey,” https://www.ndi.org/node/21520. Survey was conducted by Caucasus Research Resource Centers.
46 Web-site “Friendly Roads”: http://www.megobruligzebi.ge/
47 Online Platform “Freedom to Internet: http://www.freedomtointernet.com/
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.\(^{48}\) 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.\(^{49}\) 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.

There were no cases of charges against online users for libel or other internet activities in 2013–2014. There were also no known instances of detention or prosecution, and there were no reported occurrences of extralegal intimidation or violence against users. There have been a few cases in which civil servants were dismissed from their jobs, potentially because of their previous online activities (namely, interviews with online media representatives or posting a critical Facebook status).\(^{50}\) Officially they were fired either as a result of reorganization or intentional failure to perform duties.

There are no restrictions on the use of anonymizing or encryption tools online; however, individuals are required to register when buying a SIM card.

The Georgian Law on Operative-Investigative Activity, passed in 1999, grants the police and security services significant discretion in conducting surveillance. Police can generally begin surveillance without a court’s approval, though they must obtain it within 24 hours. There are some official requirements for launching such monitoring, but in reality, it is sufficient to label the targeted individual a suspect or assert that he or she may have criminal connections. New amendments to the law promulgated in September 2010 require that websites, email services, ISPs, and other relevant companies make private communications data such as email and chats available to law enforcement authorities when court approval is obtained.\(^{51}\)

While information regarding surveillance activities is limited, local NGO representatives, under the campaign “This Affects You Too,” have insisted that the law enforcement agencies “continue to have unlimited access to all kinds of electronic communication of citizens and to personal data kept with the telecom operators. The so-called ‘black boxes’ that are installed with the mobile operators, allow law enforcement agencies to simultaneously wiretap tens of thousands of people and determine their whereabouts, read their text messages and personal electronic correspondence sent via email, Viber, WhatsApp, BBM, and other applications.”\(^{52}\) As a response to these suspected surveillance activities, in March 2014, the group started advocating for legislative amendments.


\(^{49}\) The law is available in English on the GNCC website at: http://www.gncc.ge/index.php?lang_id=ENG&sec_id=7050&info_id=3555.


\(^{52}\) Campaign “This Affects You Too,” “Civil society against illegal surveillance: This affects you!” Announcement of the campaign representatives published on their official web-site, March 6, 2014, http://esshengexebe.ge/?menuid=10&lang=1&id=988.
to limit the infringement upon private life and abuse of power by entities carrying out secret investigative actions. They also advocated for setting up supervision mechanisms and implementing internationally-accepted standards to prevent potential systematic violations in the future. As of May 2014, the legislation had not been passed.53

Additionally, as of 2013 Georgia has a new government authority—the Personal Data Protection Inspector—who is entrusted with protecting people’s right to privacy. Even though the office of the inspector is able to investigate private companies for violations of the law, its mandate is often considered insufficient to stop the ministry of interior’s unchecked systematic surveillance of electronic communication, since it does not have access to data that is collected and processed for the purposes of public and national security (including economic security), defense, criminal investigations, or court proceedings.54 Despite these limitations, the first report on the state of personal data protection identified major challenges and deep-rooted systematic problems including: the processing of a disproportionately large amount of data without proper legal grounds; the illegal disclosure of personal information; failure to meet legal requirements related to video surveillance; and failing to limit the use of data for direct marketing campaigns (including advertisements sent via text to a user’s mobile phone without their consent and without the option to remove their number from the advertiser’s list).55

A special commission established by the parliament selected a public defender for consumer rights under the GNCC, for the purposes of enhancing mechanisms for the protection of users’ rights and building an informed society. The ombudsman is tasked with protecting the rights and interests of customers in the spheres of electronic communication and broadcasting, including discussing applications and complaints by customers and conducting administrative proceedings on cases; participating in the development of those normative acts by the GNCC which may affect the interests of customers; and representing and protecting customers’ interests in disputes with service provider authorized and/or license holder entities, in the GNCC and in court.56

ISPs and mobile phone companies are 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.

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 website57 as well as on their official Facebook page.58 Additionally,
Georgia

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. Significantly, secure DNS services enable users to automatically block harmful content by using DNS parameters offered by Cert.gov.ge.
Germany

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>4</td>
<td>4</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>17</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 80 million
Internet Penetration 2013: 84 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Free

Key Developments: May 2013 – May 2014

- Despite an endorsement by both the newly elected government and the European Parliament, the principle of net neutrality is still not entirely safeguarded (see Limits on Content).

- The newly enacted ancillary copyright law for press publishers raised concerns with regard to the right to freedom of communication and freedom of information on the internet (see Limits on Content).

- In August 2013, the Federal Court of Justice issued a ruling that further substantiated intermediary liability for content hosts whose business model facilitates copyright infringement (see Limits on Content).

- The disclosures by former NSA contractor Edward Snowden revealed the vast scale of internet surveillance in Germany by both foreign and German intelligence agencies. The federal government drew criticism for reacting too reluctantly to the revelations (see Violations of User Rights).
Introduction

The German federal elections on September 22, 2013 emphasized the fact that internet freedom issues are now a major topic on the political agenda in the country. The appointment of a minister for digital infrastructure and the establishment of a standing committee for the digital agenda within the federal parliament are a testament to this development. Additionally, the program for the current legislative session comprises policy items that range from an accelerated extension of high-speed web infrastructure, a strengthening of data protection, and civil rights on the internet.

Meanwhile, freedom of information and communication remains under pressure. Although the governing parties’ coalition agreement endorses net neutrality and the European Parliament has voted in favor of the principle, it is still not entirely safeguarded in Germany’s existing legal framework. Furthermore, the ancillary copyright law for press publishers that went into effect in August 2013 could potentially reduce the accessibility of news sources on the internet and diminish the diversity of the supply of information, though so far this legislation seems to have had minimal impact.

Like in many other countries, data protection and online privacy in Germany have become major topics of conversation due to the revelation of systematic, ongoing, and widespread online surveillance by international intelligence agencies. While the U.S. National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) are considered to be the agencies that bear the most responsibility for the intrusions into protected data and communications, reports disclosed that the German intelligence agency Bundesnachrichtendienst (BND) also carried out potentially unconstitutional surveillance against German citizens and residents. The federal government was criticized for its reluctant and apologist reaction to the scandal.

At the same time, the ongoing struggle against data retention may have gained a partial victory when, on April 8, 2014, the European Court of Justice declared the EU Data Retention Directive invalid due to disproportionate interference with the fundamental rights to respect for private life and to the protection of personal data. Despite previously stated plans to enact a national law with the goal of implementing data retention policies in Germany as a result of this decision, the federal government announced it will refrain from initiating a bill until the EU has decided on a new directive.

Obstacles to Access

Germany’s network infrastructure for information and communication technologies is well-developed, with 77 percent of the population in Germany having private internet access. Together with the number of mobile-only internet users, this has resulted in an overall internet penetration rate of 88 percent, according to Eurostat findings, which is 9 percentage points above the European Union (EU) average (the International Telecommunication Union places the internet penetration rate for Germany at 84 percent). However, growth in internet penetration is slowing, with an increase

---

The number of individuals who plan on obtaining private access remains at an unchanged 3.1 percent.3

Internet connections in private homes are nearly universal, with 95 percent of households having a connection of at least 1 Mbps.4 The most widely used mode of access is still DSL (over 81 percent), but cable internet connections are becoming more widespread (at nearly 19 percent, compared to 11 percent in 2013).5 Connections with more than 50 Mbps are available for about 58 percent of households.6 In their coalition agreement after the 2013 federal election, the Christian Democratic Union, Christian Social Union, and Social Democratic Party declared that high-speed broadband supply should be available for every citizen by the year 2018,7 a goal that was criticized as both lacking proper funding and being insufficient for a modern industrialized country.8 Regarding the take-up of connections of at least 10 Mbps, Germany is lagging internationally, with only 31 percent of households having such connections, in comparison to the EU average of 48 percent.9

Mobile phone penetration in Germany is nearly universal, with a penetration rate of over 131 percent.10 In 2013, 41 percent of online users accessed the internet via mobile devices, compared to 23 percent a year earlier.11 The number is on a par with the EU average.12 According to the Federal Ministry of Economics and Technology, Germany is ranked 8th internationally in terms of mobile internet access.13 Of all German citizens from the age of 14, 40 percent own a smartphone.14

---


3 Initiative D21, 2013, p. 10.


availability of basic UMTS connections is good (85 percent of all German households), and the coverage of fast LTE technology has grown considerably in the past year, with 70 percent of all households being covered with at least 2 Mbps, and 44 percent at 6 Mbps and above.15

There is still a gender gap when it comes to accessing the internet in Germany (over 81 percent of men use the internet compared to under 72 percent of women), but the increase of female users compared to male users was again slightly higher in 2013, resulting in a decreasing gender-difference of about 10 percentage points compared to 11 percent in 2012 and 12 percent in 2011.16 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.17

Differences in internet usage depending on formal education have not significantly changed over the past few years: the discrepancy between people with low and high levels of formal education is still about 20 percent. 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 55 percent penetration rate, whereas those with more than EUR 3,000 (US$3,848) net income have a penetration rate of 93 percent.18 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 (73 percent); however, this difference has been decreasing over the past few years.19 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 Mecklenburg-Western Pomerania has again slightly decreased and is now at around 12 to 13 percent.20 As this persisting imbalance is widely considered problematic, the elected coalition of CDU/CSU and SPD has made it a priority to increase broadband availability in rural areas.21

Prices for flat rate broadband internet have decreased in recent years and now 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 3,871 (US$4,965), and ranks below average prices in OECD countries.22 Nevertheless, as the stark differences in internet usage in relation 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

---

15 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 in cities.
16 Initiative D21, 2013, p. 22.
17 Initiative D21, 2013, p. 22.
18 Initiative D21, 2013, p. 23.
20 Initiative D21, 2013, p. 20.
21 Coalition Agreement, p. 34-5.
internet access are not adequately reflected in basic social benefits. Telecommunication services have become slightly less expensive, decreasing by about 2 percent, while the costs for mobile telecommunication services also decreased by about 2 percent between the third quarter of 2012 and the third quarter of 2013.

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 43.1 percent, though it has been in slight decline in recent years as competition has grown. Other ISPs with significant market share include 1&1-United Internet with 12.5 percent, Vodafone (as Arcor) with 10.4 percent, O2-Telefónica with 7.9 percent, and cable companies Unity Media (9 percent) and Kabel Deutschland (7.3 percent). While Deutsche Telekom’s dominant position remains unchallenged for the time being, competition is expected to grow considerably after Vodafone’s acquisition of Kabel Deutschland in October 2013.

There are four general carriers for mobile internet access: T-Mobile, Vodafone, E-Plus, and O2-Telefónica. In 2013, T-Mobile maintained its market leadership, having obtained a 33.5 percent market share compared to 32 percent a year earlier. Vodafone follows second with 28 percent, a decline by two percent since 2012. The rise of the two smaller providers, E-Plus and O2-Telefónica, has slowed: in 2013 the providers remained at a steady 21.6 and 16.8 percent, respectively. However, while the mobile market had been considered one of the most competitive in the EU, this fact might suffer a setback in view of the intended merger of O2-Telefónica and E-Plus, which would position the new company as the market leader and reduce the market to three competitors.

---


Accordingly, the EU Commission is investigating the proposed deal.\(^{32}\) Competition of mobile services in downstream markets remains limited, since most German mobile providers contractually prohibit services such as Voice over Internet Protocol (VoIP).\(^{33}\) The Body of European Regulators for Electronic Communications (BEREC) has started to investigate this widespread practice across Europe and is discussing possible regulatory interventions.\(^{34}\) The issue was also part of the European Parliament’s considerations that led to its decision on net neutrality in April 2014 (see “Limits on Content”).\(^{35}\)

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.\(^{36}\) 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 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.\(^{37}\) 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.\(^{38}\)

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.\(^{39}\) 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”\textsuperscript{40} 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.\textsuperscript{41} 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.\textsuperscript{42}

**Limits on Content**

Government blocking of websites or internet content rarely takes place in Germany.\textsuperscript{43} In 2013-2014, 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)\textsuperscript{44} indicates that private entities substantially shape the availability of online content.\textsuperscript{45} 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,”\textsuperscript{46} and consequently sues Google for damages.\textsuperscript{47} As a result of this disagreement, YouTube blocks videos for users within Germany if the video might contain copyrighted music, instead showing an error message saying that the video...


\textsuperscript{43} Due to substantial criticism by activists and NGOs that provoked an intense political debate, the 2010 law on blocking websites containing child pornography, the Access Impediment law (Zugangserschwerungsgesetz), never came into effect and was finally repealed by the German parliament in December 2011.

\textsuperscript{44} 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.de, April 9, 2014, http://www.taz.de/136441/.

\textsuperscript{45} Compared to 0.9 per cent in the United States and ca. 1 per cent in Austria and Switzerland. Cf. sueddeutsche.de, “Diese Kultur ist in Deutschland leider nicht verfügbar” [This culture is not available in Germany], January 28, 2013, http://sz.de/1.1584813.


is not available in Germany because GEMA has not granted the publishing rights. This practice results in the blocking of seemingly unrelated video content that may have copyrighted music playing on the radio in the background, for example. Google has raised concerns about the resulting undesired harms for freedom of expression.

In early 2014, most likely due to these copyright concerns, YouTube blocked a number of videos and live streams from the protests and uprisings in Ukraine, displaying the error message referring to GEMA's copyright claims. However, GEMA denied that it was in any way responsible for the blocking practice in this context, stating that YouTube's error message incorrectly implies that GEMA, not YouTube, is blocking the content. 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. Although the judgment is not final, YouTube subsequently altered the content of the displayed message on blocked videos.

New evidence has confirmed that ISPs across Europe regularly use 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. In their coalition agreement, the governing parties have announced a plan for new legislation to restrict the practice.

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.

Similarly, in another European Court of Justice ruling issued on May 13, 2014, the court found that the 1995 Data Protection Directive applied to the activities of search engines like Google, and that

48 GEMA demands 0.375 cents per retrieval.
49 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/1jFQK7.
these companies may have to remove search results if the data is deemed to violate an individual’s right to privacy. Cases in which search engines may have to remove links are limited only to searches for an individual’s name: the original content in the link would not be removed and would still appear in other searches, but the link would no longer appear in search results for the individual who requested the removal. Many critics of this ruling argue 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.

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 is used extensively. According to Google’s latest transparency report regarding requests to remove content, covering the period from January to June 2013, the company received 138 requests from the German courts and other public authorities. Based on absolute numbers, with regard to court orders Germany ranks fourth of all countries that issued requests for removal of content, following the United States, Brazil, and Turkey. Defamation remains by far the most common reason for court orders to remove content.

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.

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” (Stoererhaftung) of access providers and host providers for third party content. Although access and host providers 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

---

61 Cf. the respective § 5, Abs. 3 JMSV.
63 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).
64 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.
secondary liability. 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.

In 2012, court rulings limited the liability privilege of ISPs 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. 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.

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. As a consequence, host providers are required to monitor their own servers and search for copyright-protected content as soon as it has been notified of a possible violation. In their coalition agreement, the governing parties announced that such host providers should lose the privilege and the ability to obtain advertising revenues through their business practices. However, provider liability has to be in line with the European legal framework, in this case, the Directive 2000/31/EC.

The situation regarding intermediary liability was further complication by a European Court of Human Rights (ECtHR) case regarding third-party comments. On October 10, 2013, the ECtHR issued a ruling that reaffirmed an earlier Estonian Supreme Court decision regarding the legal liability of content hosts for third-party comments. 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.

65 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.
71 Coalition Agreement, p. 93.
ISPs are obliged to disclose customer information for prosecutions of copyright infringement, even though the person may not have infringed copyrights for commercial purposes.\(^{74}\) 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.\(^{75}\) Whereas linking to other websites is regarded as unproblematic, embedding content, primarily videos from other sources, could cause liability risks for the provider.\(^{76}\)

An important exception to the liability privilege concerns wireless networks.\(^{77}\) Because of a highly disputable ruling against the existing liability privilege by the Federal High Court in 2010, legislative initiatives from states and political parties now seek to modify the secondary liability of local Wi-Fi operators. In this respect, the governing parties 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.\(^{78}\) However, while the general intention has been lauded, questions remain concerning the details of such a legal framework.\(^{79}\)

The principle of proportionality has constitutional status in Germany to which public authorities must comply. The interplay between the Ministry of Justice, the Federal Data Protection Officer, the association of internet service providers (Eco), and the internet community effectively hold the bodies involved accountable.

There is no systematic self-censorship in the German media. Still, there are more or less unspoken rules reflected in the publishing principles of the German press.\(^{80}\) The penal code and the JMStV prohibit content in a well-defined manner (such as child pornography, racial hatred, and the glorification of violence).

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 April 2013, the Federal Ministry of Defense took legal steps against a newspaper,\(^{81}\) demanding that it delete a set of leaked mission reports covering Afghanistan operations of the federal armed forces (Bundeswehr), based on alleged copyright

---


\(^{75}\) LG Hamburg [Regional Court Hamburg], judgement of May 18, 2012, Az. 324 O 596/11, http://openjur.de/u/404386.html.


\(^{77}\) 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 Huffington Post (blog), June 8, 2010, http://www.huffingtonpost.com/christopher-burgess/three-good-reasons-to-loc_b_599945.html.

\(^{78}\) Coalition Agreement, p. 35.


infringement. The same legal argument was employed by the Federal Ministry of the Interior in January 2014 after the website FragdenStaat.de 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.

The principle of net neutrality was legally codified with the latest amendment of the telecommunications act (Telekommunikationsgesetz, TKG), § 41a TKG, enacted in May 2012. The law authorizes the government to define basic requirements for non-discriminatory data transfer and content access, but it does not require the government to take any further action. The German Federal Network Agency (Bundesnetzagentur, BNetzA) principally supports net neutrality, but instead of safeguarding it legally, the national regulator favors new business models based on price discrimination and differentiated classes of service as long as ISPs are transparent about their policies and give customers a choice.

The lack of concrete action on the part of the German government was met with criticism when the market-leading telecommunications company Deutsche Telekom announced plans to place limits on customers’ high-speed data transfer per month while exempting certain services such as their own movie-streaming and television offers. Afterward, the Federal Ministry of Economy and Technology presented two drafts of a net neutrality decree (Netzneutralitätsverordnung) in June and July 2013. However, German consumer advice centers (Verbraucherzentralen) raised concerns regarding the administrative proposal’s effectiveness concerning net neutrality. In October 2013, a regional court in Cologne decided that Deutsche Telekom’s plans were unlawful at least vis-à-vis those customers who had entered into a contract with the company that expressly included flat rate billing. Deutsche Telekom subsequently announced that it would accept the ruling, although without entirely abandoning plans to introduce differentiated classes of service in the future.

In their coalition agreement, the governing parties announced plans to make promoting and securing net neutrality a principal goal of the internet policies in the forthcoming legislative term. Still, the
declaration has been criticized as being partly inconsistent and insufficient.\textsuperscript{92} Furthermore, while the European Parliament’s April 2014 vote in favor of net neutrality has widely been considered a success, the details of the new regulation are likewise considered deficient and incomplete.\textsuperscript{93}

Germany is home to a vibrant internet community and blogosphere. 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 (\textit{Leistungsschutzrecht für Presseverleger}), a regulation that came into effect on August 1, 2013 and that would allow publishers to monetize even the small snippets of information that search engine operators display as part of the results of a query,\textsuperscript{94} raised concerns regarding the constitutionally protected rights to freedom of expression and freedom of information.\textsuperscript{95} In an advisory opinion, the Max Planck Institute for Intellectual Property and Competition Law warned that the law could lead to a decline in online diversity of available press publications and other sources of information, thus infringing on the right to communication.\textsuperscript{96} Despite coming into effect on August 1, 2013, however, search engines have not yet been impacted by the law, as no companies have taken action to enforce the copyright protection.\textsuperscript{97}

A potential downside of the rising power of internet-enabled discourse became apparent in late 2013 when a high school teacher initiated an online petition on the platform openPetition aimed at thwarting a planned curriculum change in the state of Baden-Württemberg that had the goal of promoting awareness of sexual diversity and to prevent homophobia and other forms of sexual discrimination.\textsuperscript{98} The petition quickly gained traction on the net, gathering more than 190,000 signatures within two months, a turnout that was at least in part a result of the easy accessibility of this form of activism.\textsuperscript{99} The case gave rise to concerns about the potential ramifications of online platforms for political grassroots campaigning that can have negative impacts on minority

populations. However, at the same time, opposition against the petition and its proponents’ discriminatory tendencies also quickly formed online, with the Twitter hashtag #idpet providing a tenacious forum for promotion of equality. Additionally, activists have been waging Europe-wide online campaigns in the fight for net neutrality. The vote of the European Parliament in favor of net neutrality has partly been accredited to the persistent activism.

Violations of User Rights

The NSA surveillance revelations that began in June 2013 have had a significant impact on discussions in Germany surrounding privacy, data retention, and freedom of expression online. After initial hesitation and following substantial public pressure, the federal government and public authorities have reluctantly started to review the incidents and have initiated preliminary arrangements that aim to safeguard civil rights and constrain the powers of both domestic and foreign intelligence agencies. However, no tangible, long-term solutions regarding online surveillance have been proposed as of yet.

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.

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. Furthermore, in December 2013 several political bloggers reported that the press office of the Federal Parliament had refused to grant them one-year


105 See http://www.djv.de/startseite/service/mitgliederservice/presseausweis.html.

accreditations, thus provoking allegations of discrimination against online journalists. After vocal protests, including from members of parliament, the accreditation policy was changed, although the office insisted that the principal distinction all along had merely been between professional and non-professional journalists, with only the former being eligible.

The German Criminal Code (StGB) includes a paragraph on “incitement to hatred” (§ 130 StGB), which penalizes calls for violent measures 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.

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. 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, in their coalition agreement, the elected governing parties expressly endorsed the principles of anonymity and pseudonymity, and declared the intention to further advance the techniques necessary for their effective implementation. Still, the announcement was criticized as being partly contradictory to other envisaged policies such as data retention, the implementation of which had been an officially stated goal of the coalition prior to the European Court of Justice’s decision to invalidate the EU Data Retention Directive in April 2014, thus casting lasting doubt on the federal government’s sincerity concerning the right of anonymity and pseudonymity online.

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. 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.

109 Cf. fn. 54.
112 Coalition Agreement, p. 104.
Germany

Excessive interceptions by secret services formed the basis of a 2008 Federal Constitutional Court ruling, which established a 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.” 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. 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 June 2013, documents leaked by former NSA contractor Edward Snowden revealed that the intelligence services of the United States and the United Kingdom, principally the National Security Agency (NSA) and the Government Communications Headquarters (GCHQ), had been conducting worldwide surveillance of online communications. Through the course of the revelations, the vast degree of the spying measures became apparent, culminating in the information that the NSA had considered Germany a “target state,” entailing the monitoring of about half a billion telephone, email, and text message communications in Germany each month. In the beginning of August 2013, media outlets reported that it had in fact been the German Federal Intelligence Service (Bundesnachrichtendienst, BND) which had forwarded the relevant data to the NSA since 2007. A few months later, it was disclosed that the BND had accessed internet traffic in Germany by tapping into a central node in Frankfurt, with the approval of both the Office of the Federal Chancellor and the Federal Ministry of the Interior. The practice was widely considered unlawful, as the relevant G-10 law only permits the BND to monitor international, as opposed to domestic, telecommunications. The revelation gave rise to doubts concerning the effectiveness of judicial and parliamentary control over the intelligence service.

Germany

The Federal Government was criticized for reacting too slowly to the disclosures, and even defending the services’ conduct. In particular, then Federal Minister of the Interior Hans-Peter Friedrich came under pressure after stating that a “fundamental right of security” effectively takes precedence over other constitutionally protected rights such as freedom of communication and the protection of privacy. Still, in their coalition agreement, the governing parties announced they would move forward with an international treaty to protect the citizens from excessive surveillance. However, the conclusion of a desired bilateral accord with the United States failed due to resistance from the U.S. government. After notable public pressure, in February 2014 Federal Prosecutor General Harald Range announced he would initiate a formal criminal investigation against the NSA, though only two months later, reports were released stating that instituting an official case seemed unlikely due to a lack of evidence against the agency. In March 2014, the Federal Parliament appointed a commission of inquiry to investigate the activity of the intelligence agencies of all so-called “Five Eyes” countries, as well as the role of the Federal Government, in the surveillance of communications data.

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

124 Coalition Agreement, p. 104.
Germany

which found that in the majority of cases a review by a judge does not take place.\footnote{Two independent studies from the by 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 Gusy, 2003) and Max-Planck-Institut Institute for Foreign and International Criminal Law (Hans-Jörg Albrecht, Claudia Dorsch, Christiane Krüpe 2003: 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.mpg.de/868492/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.} 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.\footnote{Breyer, Patrick, “Verfassungsbeschwerde gegen Bestandsdatenauskunft eingereicht” [Constitutional complaint against stored data inquiry submitted]. July 1, 2013, http://bestandsdatenauskunft.de/?p=357.}

In the aftermath of the enactment on the federal level, several German states established their own laws, with one state legislation even entirely omitting the requirement of preceding judicial review.\footnote{Stefan Krempl, “Länder verabschieden neue Regeln zur Bestandsdatenauskunft” [States enact new rules concerning stored data inquiries], heise.de, June 22, 2013, http://www.heise.de/newsticker/meldung/Laender-verabschieden-neue-Regeln-zur-Bestandsdatenauskunft-1894865.html.}

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 23,687 orders for telecommunications interceptions in 2012, compared to 21,118 in 2011, of which 4,488 concerned internet communications, compared to only 1,345 in the year before.\footnote{Bundesamt für Justiz [Federal Office of Justice], “Übersicht Telekommunikationsüberwachung (Maßnahmen nach §100a StPO) für 2012”, October 24, 2013 [Summary of telecommunication surveillance for 2012] http://bit.ly/1lliOCT.} There were also a total of 18,026 orders requesting internet traffic data in 2012, compared to 14,153 in 2011.\footnote{Bundesamt für Justiz, “Übersicht Verkehrsdatenerhebung (Maßnahmen nach § 100g StPO) für 2012” [Summary of traffic data collection for 2012], August 1, 2013, http://bit.ly/1lohtaru.}

Surveillance measures conducted by the secret services under the Act for Limiting the Secrecy of Letters, the Post, and Telecommunications exceed these figures. For 2012, the competent Parliamentary Control Panel reported that a total of 851,691 telecommunications – most of them email – were scanned, of which only 288 were considered relevant.\footnote{These are aggregated figures related to the three areas of risk in which scannings took place according to the report of the Parliamentary Control Panel. Cf Deutscher Bundestag, Drucksache 18/218, December 19, 2013, p.7, http://dip21.bundestag.de/dip21/btd/18/002/1800218.pdf. Note that the annually presented numbers do not refer to the last year but to the year before, i.e. 2012. 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. See also: http://www.bundestag.de/htdocs_e/bundestag/committees/bodies/scrutiny/index.html.} The panel highlighted the steady decline in surveillance measures, the number of which had been above 2.8 million in 2011. 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.\footnote{Cf. the report of the Parliamentary Control Panel: Deutscher Bundestag, Drucksache 18/218, December 19, 2013, p. 7, http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf.}

Recent evidence shows that German police authorities regularly make use of radio cell queries

\footnote{131  Two independent studies from by 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 Gusy, 2003) and Max-Planck-Institut Institute for Foreign and International Criminal Law (Hans-Jörg Albrecht, Claudia Dorsch, Christiane Krüpe 2003: 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.mpg.de/868492/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.}


\footnote{135  Bundesamt für Justiz, “Übersicht Verkehrsdatenerhebung (Maßnahmen nach § 100g StPO) für 2012” [Summary of traffic data collection for 2012], August 1, 2013, http://bit.ly/1lohtaru.}

\footnote{136  These are aggregated figures related to the three areas of risk in which scannings took place according to the report of the Parliamentary Control Panel. Cf Deutscher Bundestag, Drucksache 18/218, December 19, 2013, p.7, http://dip21.bundestag.de/dip21/btd/18/002/1800218.pdf. Note that the annually presented numbers do not refer to the last year but to the year before, i.e. 2012. 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. See also: http://www.bundestag.de/htdocs_e/bundestag/committees/bodies/scrutiny/index.html.}

for criminal investigation. The state government of North Rhine-Westphalia has conceded that between December 2010 and August 2013, the state's law enforcement authorities employed the method 10,330 times, which equates to more than 10 radio cell queries each day. Projected onto the Federal Republic of Germany, this would mean more than 50 queries every day. The extensive use of radio cell queries has raised questions of proportionality. In May 2013, members of the group of Die Linke in the Saxon parliament filed a constitutional complaint to the Federal Constitutional Court in reaction to the allegedly disproportionate employment of radio cell queries during an anti-Nazi demonstration in Dresden in February 2011. According to reports, the measures had gathered call detail records and other data of almost 60,000 people, disregarding whether they had participated in the demonstration or not.

For the sake of transparency, Germany's biggest ISP, Deutsche Telekom, has started to inform the public about the number of requests from authorities regarding stored and traffic data, IP address identification, and telecommunications interceptions. According to the report, in 2013 the provider enabled 49,796 telecommunications interceptions and disclosed 436,331 sets of traffic data and 28,162 sets of stored data. The authorities also requested the identification of 946,641 IP addresses. However, while the disclosure has been lauded in principle, its content was criticized due to the lack of detail. According to Green Party member Malte Spitz, traffic data inquiries include radio cell queries, which means that one set potentially includes thousands of individual traffic data, thus rendering the report insufficiently transparent concerning this aspect, with the effect that the extent of surveillance is in fact downplayed.

In May 2013, then Federal Commissioner for Data Protection and Freedom of Information Peter Schaar disclosed that certain offices of the agency for labor had considered investigating the behavior of unemployed persons via social media such as Facebook in order to match their

---

statements toward the authorities.\textsuperscript{147} Agency officials denied that the practice was in fact being pursued, while Schaar publically stated that it would be illegal.\textsuperscript{148} For the purpose of discovering welfare fraud, the agency furthermore called for the enactment of a statutory basis for allowing online investigations into the conduct of welfare recipients’ more generally.\textsuperscript{149} The Pirate Party contested the constitutionality of the proposed framework.\textsuperscript{150}

On April 8, 2014, after both the Irish High Court and the Austrian Constitutional Court had asked for a preliminary ruling on the validity of the EU Data Retention Directive, the European Court of Justice declared the directive to be invalid due to its disproportionate interference with the fundamental rights to respect for private life and to the protection of personal data.\textsuperscript{151} Although the Federal Ministry of Justice had reportedly already finalized a draft for a new law on data retention,\textsuperscript{152} the government declared that it did not intend to enact any regulation prior to the issuing of a new EU directive on the matter.\textsuperscript{153} So far, it is unclear whether or when the EU Commission will propose an amended directive.\textsuperscript{154} Furthermore, the ECJ judgment is likely to have a significant impact on the drafting process of a new EU Data Protection Directive. According to independent scholars, to be in line with the Court’s findings, the proposed directive will need to include, among other things, precise rules on public-private cooperation in the law enforcement sector, independent oversight, and the permitted time period of potential data retention.\textsuperscript{155}

According to a recent survey, 30 percent of all companies in Germany were victims of cyberattacks within the last two years. Of those attacks, 30 percent were conducted via the internet, while 58 percent were carried out with the help of flash drives or other devices by persons in direct contact with the attacked computer or network.\textsuperscript{156} A particularly critical cyberattack was reported in April 2014, when the German Aerospace Center (\textit{Deutsches Zentrum für Luft- und Raumfahrt}) disclosed

\begin{itemize}
\item \textsuperscript{147} Pascal Beucker/Anja Krüger, “Der Arbeitsagentur gefällt das” [The agency for labor likes this], taz.de, May 24, 2013, \url{http://www.taz.de/116813/}.
\item \textsuperscript{148} Achim Sawall, “Jobcenter sollen nicht bei Facebook recherchieren” [Job centers ought not investigate on Facebook], golem.de, May 24, 2013, \url{http://www.golem.de/news/bundesdatenschuetzer-jobcenter-sollen-nicht-bei-facebook-recherchieren-1305-99432.html}.
\item \textsuperscript{149} Spiegel Online, “Internethandel: Arbeitsagentur will Hartz-IV-Empfänger im Netz überwachen” [Internet trading: agency for labor wants to monitor welfare recipients on the net], November 14, 2013, \url{http://www.spiegel.de/wirtschaft/soziales/arbeitsagentur-will-hartz-iv-empfaenger-im-netz-ueberwachen-a-933520.html}.
\item \textsuperscript{150} Pirate Party, “Verdachtsunabhängige Überwachung von Alg II-Empfängern gefährdet Rechtsstaat” [Surveillance of welfare recipients without suspicion threatens the rule of law], press release, November 14, 2013, \url{https://www.piratenpartei.de/2013/11/14/verdachtsunabhaengige-ueberwachung-von-alg-ii-empfaenern-gefaehrdet-rechtsstaat/}.
\item \textsuperscript{152} Kai Biermann, “Gerichtshof kippt Richtlinie zur Vorratsdatenspeicherung” [European Court of Justice declares Data Retention Directive as invalid], Zeit Online, April 8, 2014, \url{http://www.zeit.de/digital/datenschutz/2014-04/vorratsdatenspeicherung-europaeischer-gerichtshof-eugh}.
\item \textsuperscript{153} Ingo Pakalski, “Vorerst kein neues Gesetz zur Vorratsdatenspeicherung” [No new law on data retention for the time being], golem.de, April 14, 2014, \url{http://www.golem.de/news/bundesregierung-vorerst-kein-neues-gesetz-zur-vorratsdatenspeicherung-1404-105837.html}.
\item \textsuperscript{155} Franziska Boehm and Mark D. Cole, “Data Retention after the Judgement of the Court of Justice of the European Union”, Münster/Luxembourg, 30 June 2014, \url{http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole - Data Retention Study - June 2014.pdf} p. 84-87.
\item \textsuperscript{156} BITKOM, “Fast ein Drittel der Unternehmen verzeichnet Cyberangriffe” [Almost a third of all companies registers cyberattacks], press release, March 11, 2014, \url{http://www.bitkom.org/de/presse/8477_78903.aspx}.
\end{itemize}
that for months it had been attempting to fend off a very elaborate and sophisticated cyberattack that had allegedly been carried out by a foreign intelligence service. Among other things, the Center conducts research in defense technologies.\textsuperscript{157}

In response to the rising number of attacks, the Federal Ministry of Interior published a “Cyber Security Strategy for Germany” in 2011.\textsuperscript{158} In March 2013, the Federal Ministry of the Interior proposed a law 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).\textsuperscript{159} The Federal Ministry of Economics and Technology blocked the legislative draft in the early consultation phase. Digital rights advocates criticized the legislative proposal because it did not include a notification of users in instances of security breaches. Industry associations, on the other hand, feared potential costs and bureaucratic burdens of notifying the Federal Office for Information Security.\textsuperscript{160} Despite these reservations, in their coalition agreement the governing parties announced intentions to further promote such a law,\textsuperscript{161} aiming for enactment before mid-2015.\textsuperscript{162}

\begin{itemize}
\item \textsuperscript{157} Spiegel Online, “Cyber-Angriffe: Spähangriff auf Deutsches Luft- und Raumfahrtzentrum” [Cyberattacks: espionage intrusions into German Aerospace Center], April 13, 2014, \url{http://www.spiegel.de/netzwelt/web/dlr-mit-trojanern-von-geheimdienst-ausgespaehlt-a-964099.html}.
\item \textsuperscript{159} Cf. Federal Ministry of the Interior, “Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme” [Draft legislative proposal for improving the security of information networks], March 5, 2013, \url{http://bit.ly/XsVWs1}.
\item \textsuperscript{161} Coalition agreement, p. 103.
\item \textsuperscript{162} Christian Raum, “IT-Sicherheitsgesetz: staatliche Kontrolle und höhere Kosten” [IT security law: governmental control and higher costs], ZDNet, March 10, 2014, \url{http://www.zdnet.de/88186435/it-sicherheitsgesetz-staatlich-kontrolle-und-hoehere-kosten/}.
\end{itemize}
Hungary

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>5</td>
<td>5</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>10</td>
<td>11</td>
</tr>
<tr>
<td><strong>TOTAL</strong> (0-100)</td>
<td>23</td>
<td>24</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 9.9 million

Internet Penetration 2013: 73 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: No

Bloggers/ICT Users Arrested: No

Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- Revisions to the criminal code, which came into effect in July 2013, require ISPs to block content deemed illegal by a court order. Websites hosting illegal content are placed on a non-public “blacklist” operated by the National Media and Infocommunications Authority (NMHH) (see **Limits on Content**).

- On November 5, 2013, the criminal code was modified to make defamatory video or audio recordings punishable by up to three years in prison (see **Violations of User Rights**).
Introduction

Over the past four years, new laws regulating the media, including online media outlets and news portals, have caused significant concern among civil liberties advocates and the international community.¹ The National Media and Infocommunications Authority (NMHH) and its decision-making body, the Media Council, were established in 2010 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 modifications to the media laws in May 2012 based on the December 2011 ruling of the Hungarian Constitutional Court, 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.² In particular, high fines can be imposed on all types of media outlets by the single-party Media Council based on an obscure content provision.

Over the past year, new modifications to the criminal code have further restricted the environment for internet freedom in the country. Of particular concern is an amendment passed in November 2013 that introduces criminal penalties for publishing defamatory video or audio recordings. The most severe penalties relate to content that is published to a “wide audience,” causing concerns that this amendment will have a significant impact on media outlets.

Despite the increase in restrictive laws, over the past decade the availability of broadband connections has increased, and a majority of the population is online. Information and communication technologies (ICTs) are being used not only for social activities and newsgathering, but also increasingly for political activism.

Obstacles to Access

Internet penetration rates for Hungary vary according to the source. In 2012, the Hungarian Central Statistical Office reported that 68 percent of households had broadband internet connection, up from 61 percent in 2011.³ According to the International Telecommunication Union (ITU), internet penetration in Hungary stood at nearly 73 percent in 2013, compared to 61 percent in 2008,⁴ while

---

the National Media and Infocommunications Authority of Hungary (NMHH) reported in late 2013 that there were almost 2.3 million broadband internet subscriptions in a country of 10 million inhabitants. Dial-up internet service is not widely used. The NMHH recorded a mobile phone penetration rate of about 117 percent and nearly 4 million mobile internet subscriptions. In 2012, only 26 percent of the population had never used the internet, a decrease from 52 percent in 2006. A 2011 Eurobarometer survey found that Hungarian households that do not have internet subscriptions cite reasons including: monthly subscriptions are too expensive, the cost of buying a computer and modem are too high, or that no one in the household has an interest in using the internet.

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 2012–2013 data from the Millward Brown research company, internet penetration in Hungary was over 89 percent among those living under the best circumstances, compared to merely 43 percent among those living under the worst circumstances. Internet penetration was over 75 percent among the employed and 46 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 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. A recent survey found that the IT infrastructure in Hungarian public schools is poor compared to the European Union average. Hungary has the lowest rate of students in schools with electronic educational resources, while the majority of schools have a broadband speed under 10 Mbps.

In late 2012, most internet users accessed the internet primarily from home or work, while access at internet cafes and “telecottages” (local community centers) was less common; the use of

9 Special Eurobarometer 362, “E-communications household survey” (Eurobarometer, July 2011): 56.
10 Millward Brown TGI Magyarország 2012/3-4 2013/1-2 quarter.
devices such as smartphones and tablets increased. In early 2013, industry experts estimated that approximately 2.4 million people were using smart phones. An increasing number of widely-used software and websites are available in Hungarian, and there are several Hungarian blog-hosting sites. By late 2013, there were more than 637,000 registered ".hu" domains recorded at some 150 domain name registrars.

The government does not restrict bandwidth, routers, or switches, and backbone connections are owned by telecommunications companies rather than the state. Legally, however, 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 maintains the Hungarian internet traffic between domestic internet service providers (ISPs), and is overseen by the Council of Hungarian Internet Service Providers (ISZT) without any governmental interference.

Three ISPs control over 50 percent of the total fixed broadband market, and there are three mobile phone service providers, all privately owned by foreign companies. The existence of only three mobile phone service providers (in 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. A state-owned consortium tried to enter the market in 2012, but after the tender was brought to court, the project was abandoned.

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, and the government withdrew the special tax levied in 2010. However, another tax was introduced in mid-2012 on mobile phone calls and text messages.

---

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.  
$3 monthly for individual subscribers)\textsuperscript{27} to counterbalance the withdrawal of the special tax of 2010. Almost all mobile service providers have since raised their prices.\textsuperscript{28}

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 governing two-thirds parliamentary majority.\textsuperscript{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.\textsuperscript{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 a few applicants, who received a large share of the available frequencies.\textsuperscript{31}

With the recently adopted Fundamental Law of Hungary, in operation since 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 arbitrary grounds,\textsuperscript{32} calling into question the independence of the agency.

## Limits on Content

The recently accepted changes to the civil and penal codes somewhat alter the regulatory landscape when it comes to online content, imposing limitations principally in the name of child protection. There is no sign of the government mandating any systematic filtering of websites, blogs, or text messages. Online content is somewhat limited as a result of self-censorship, lack of revenue for independent media outlets online, and the dominance of the state-run media outlet. The government does not place any restrictions on access to social media and communication applications: YouTube, Facebook, Twitter, Tumblr, international blog-hosting services, instant messaging, person-to-person communication, and other applications are freely available.


\textsuperscript{28} “Telefonadó: A Telenor és a Magyar Telekom is emeli a díjait”, [Telephone tax: both Telenor and Magyar Telekom raises prices], Hvg.hu, September 10, 2013, http://hvg.hu/gazdasag/20130910_Vandorlasba_kezdhet_a_mobilpiac.

\textsuperscript{29} Act CLXXXV of 2010, Art. 124.

\textsuperscript{30} Act CLXXXV of 2010, Art. 111/A.


\textsuperscript{32} Act CXII of 2011 on data protection and freedom of information, Section 40, par. 1, 3; Section 45, par. 4–5, http://www.naih.hu/files/ActCXIIof2011_mod_2012_05_09.pdf.
By the end of November 2013, the parliamentary majority accepted a modification to a set of laws in the name of child protection that urges ISPs to provide filtering software on their websites for free for subscribers to use in their homes; however, institutions such as public libraries and public schools will be urged to use such filters to protect children and to provide their “mental, physical and intellectual development” – as the explanation of the draft highlights. The modifications became effective as of January 1, 2014.

The new penal code, which took effect in 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. The list, referred to as KEHTA (Hungarian acronym for “central electronic database of decrees on inaccessibility”), went into effect on January 1, 2014 with the primary aim of fighting against child pornography, crimes against the state, and terrorism. 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. As of May 2014, there is no evidence that the law has been applied to block any online content.

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. Intermediaries are also not obliged to verify the content they transmit, store, or make available, nor do they need to search for unlawful activity. Intermediaries are required to make data inaccessible, either temporarily or permanently, once they receive a court order stating that the hosted content is illegal. 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.” The law fails to clarify what editorial responsibility entails and whether it

---

33 Act C of 2003 on electronic communication, Art. 149/A.
34 Act C of 2012, Art. 77.
35 Act XXXVIII of 1996 on International Assistance in Criminal Matters, Art. 60/H.
36 Act C of 2003 on electronic communication, Art. 159.
40 Act CVIII of 2001, Art. 7. par. 3.
42 Act CIV of 2010, Art. 1, par. 6.
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.  

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 was harmed in his right to good reputation, and that the defendants needed to pay for the legal expenses incurred.

The legal implications of comments posted online were further substantiated by a judgment of the Constitutional Court in 2014. In May 2014, the Constitutional Court issued a ruling stating that the publisher bears responsibility for comments posted on a given website. Dunja Mijatovic, the OSCE Representative on Freedom of the Media warned that the judgment may curb freedom of expression. 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.

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.” Further, the law states that constitutional order and human rights must be respected, and that public morals cannot be violated. 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 $111,000). 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. Any such action can be appealed in court, although the 2011 overhaul of the judiciary calls into question the independence of the court system.

A series of interviews conducted with journalists in 2012 illustrate the extent of self-censorship in Hungary, which is a result of political and economic pressure on both traditional and online media outlets. According to most of the interviewees, the media laws had not made any difference when it came to self-censorship; instead, as one respondent noted, “the two-third majority push of executive power, the unprecedented leverage of that power, and the rise of the Fidesz party” have had a

---


49 Act CIV of 2010, Art. 16, and Art. 4, par. 3.

50 Act CLXXXV of 2010, Art. 186, par. 1, 187, par. 3. bf.

51 Act CLXXXV of 2010, Art. 187, par. 3. e, 189, par. 4.
greater effect on self-censorship. Another journalist added that “party finance is entangled with media financing. Political and economic influence is exerted through public and private advertising.” A respondent explained that “there was always some other interest at play, political or from the side of business and advertising—or both simultaneously, because these two often go hand in hand.”

A respondent explained that “there was always some other interest at play, political or from the side of business and advertising—or both simultaneously, because these two often go hand in hand.”

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.”

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 same phenomenon is seen in the case of other platforms such as radio stations and outdoor advertisements: companies with close ties to the governing party received a large share of state funding for advertisements in 2012. However, there is currently no coherent data to determine the level of political influence over advertisements in cases of online media. 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.

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

---


59 “Leépítés a Stop.hu-nál” [Redundancies at Stop.hu], Index.hu, July 4, 2013, http://index.hu/kultur/media/2013/07/04/leepites_a_stop.hu-nal/.

Hungary

continuously published lists of public fund misuse by politicians, though such efforts have resulted in few consequences given the publication’s limited reach.

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.61

Although MTI has a major effect on traditional and online content, the online content landscape is relatively diverse. The two main news portals are Origo.hu and Index.hu.62 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, for the minority Roma community;63 the LGBTI community and religious groups have online resources and forums as well. 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.64 Trolling is usually moderated where it is possible to comment on 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.65 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.66

Facebook, which had almost 4.8 million users in Hungary as of December 2013,67 has grown increasingly popular as a tool for advocacy, especially after the 2010 parliamentary elections.68 Since then, many Facebook groups have been created, and several large demonstrations were organized and disseminated through Facebook, mobilizing tens of thousands of people both

---

64 To name a few: Atlatszo.hu, K-monitor.hu, Mandiner.hu, Szuveren.hu, Velemenyvezer.blog.hu, and the sites of Human Civil Liberties Union (Tasz.hu), Eötvös Károly Institute (Ekint.org) and Fizettem.hu.
for and against the government. In 2013, protests organized online and other civil initiatives continued for various social and political issues. Protests are frequently broadcast online using Ustream, and pictures and videos are distributed instantly via Facebook. Milla (One Million for Press Freedom), one of the organizations creating Together 2014, a group aiming at defeating the Orbán administration in the 2014 parliamentary elections, is a grassroots movement founded on Facebook in response to the 2010 media laws that has since grown to be one of the largest opposition movements, organizing numerous demonstrations.

**Violations of User Rights**

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 international actors for threatening freedom of expression and for targeting the media, given that the longest sentence applies to materials that are widely published.

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, partly regarding the independence of the National Agency for Data Protection and the judiciary. The Court of Justice of the European Union referred the case of the data protection authority to the European Data Protection Supervisor. The European Commission expressed concerns over Hungary’s decision to lower the mandatory retirement age from 70 years to 62 years

---


71 “Hungarian constitution is ‘not a toy’,” Marietta Le, March 7, 2013, http://globalvoicesonline.org/2013/03/07/hungarian-constitution-is-not-a-toy/


76 Act C of 2012, Articles 226/A and 226/B.


81 Case C-288/12, Commission v Hungary, October 12, 2013.
for judges and prosecutors, effectively sending 274 judges, including some on the Supreme Court, into early retirement.\textsuperscript{82} In November 2012, the Court of Justice of the European Union ruled that the early retirement of judges, prosecutors, and notaries was discriminatory.\textsuperscript{83} Prior to that, in July 2012, the Hungarian Constitutional Court ruled that the early retirement provision was unconstitutional.\textsuperscript{84} 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.\textsuperscript{85}

Another debated issue is related to a provision in the new civil code, which stipulates that a photographer must obtain permission from the subjects in the picture when taking press photos (except at public events).\textsuperscript{86} 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.\textsuperscript{87} 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.\textsuperscript{88}

In May 2013, the parliamentary majority modified the freedom of information act\textsuperscript{89} within the span of two days to restrict the accessibility of public data, claiming that some of the requests were “excessive.”\textsuperscript{90} 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 remained ambiguous and left 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.\textsuperscript{91}

The new civil code (Act V of 2013), which came into effect on March 15, 2014, enables any member of a national, ethnic, racial or religious group to enforce their personal rights.\textsuperscript{92} Some experts claim that this will cause a landslide of court cases, as anyone can file a civil proceeding claiming that he or she belongs to a certain group. Anyone harmed in his or her personal rights can ask the court to

\begin{itemize}
\item \textsuperscript{82} “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.
\item \textsuperscript{83} Judgment of the Court (First Chamber), Case C-286/12, November 6, 2012, \url{http://bit.ly/14TsXJ}
\item \textsuperscript{84} “Elkaszálta a bírói nyugdíjszabályt” [The retirement rule for judges was annulled], Index.hu, July 16, 2013, \url{http://index.hu/bejold/2012/07/16/elkaszaltak_a_biroi_nyugdijszabalyt/}
\item \textsuperscript{85} “Megszavazták a bírói nyugdíjba küldését” [The law on the slow retirement of judges was accepted], Hvg.hu, March 11, 2013, \url{http://hvg.hu/itthon/20130311_Megszavaztak_a_birak_lassu_nyugdijba_kuld}.
\item \textsuperscript{86} Act V of 2013 on the civil code, Art. 2:48.
\item \textsuperscript{87} “Az új Polgári Törvénykönyv és a sajtófotó,” [The new civil code and the press photo], Cij.hu, June 18, 2013, \url{http://www.cij.hu/az-uj-polgari-torvenykonyv-es-a-sajtofoto}.
\item \textsuperscript{88} Daniel Nolan, ‘Hungary law requires photographers to ask permission to take pictures,’ Theguardian.com, March 14, 2014, \url{http://www.theguardian.com/world/2014/mar/14/hungary-law-photography-permission-take-pictures}.
\item \textsuperscript{89} Act CXII of 2001 on informational self-determination and freedom of information.
\item \textsuperscript{90} Marietta Le, “Hungary: Government limits FOIA transparency law,” Global Voices, May 8, 2013, \url{http://advocacy.globalvoicesonline.org/2013/05/08/hungary-government-limits-foia-transparency-law/}.
\item \textsuperscript{91} “Transparency international turns to higher authorities,” Transparency International, July 3, 2013, \url{http://www.transparency.hu/Transparency Internacional turns to higher authorities?bind_info=index&bind id=0}.
\item \textsuperscript{92} Act V of 2013, Art. 2:54, par. 5.
\end{itemize}
declare that he or she was harmed, to place a ban on the unlawful activity, to claim a damnification fee for the non-pecuniary damages caused, or to claim compensation.93

Critics of the 2010 media laws contend that the Media Council operates with unclear provisions and imposes high fines and sanctions on media outlets,94 which might give rise to uncertainty and fear, lead to self-censorship, and have a chilling effect on journalism as a whole. As of December 2013, no online media outlet had been penalized for violating the new stipulations introduced by the 2010 media laws, and 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.”95 In May 2012, the parliament modified the media regulation, ostensibly in order to comply with the ruling of the Constitutional Court,96 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.”97

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 shall be punished by imprisonment of up to one year.98 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.99 However, in February 2013, the Constitutional Court ruled the ban on using totalitarian symbols unconstitutional,100 though the parliamentary majority decided to include it again in revisions to the penal code in April 2013.

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 The new civil code introduced 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

---

101 Bill Nr. T/7971 on the Civil Code, Art. 2:45.
102 Bill Nr. T/7971, Art. 2:52–53.

368 www.freedomhouse.org
discussion of public affairs in cases where the human dignity of a public figure is violated. 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.

Prior to 2008, the penal code was rarely used in cases of defamation or slander. More recently, criminal investigations of online activities have become a growing phenomenon. In November 2012, the police launched an investigation based on comments that appeared on Nepszava.hu and the news site Hir24.hu 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 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. 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. The penal proceeding is still pending.

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 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. This was the first case since the democratic transition in which someone has 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.

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.\textsuperscript{113} Additionally, to sign a contract with a mobile phone company, users must provide personal data upon purchase of a SIM card.\textsuperscript{114} Encryption software is freely available without government interference; Pretty Good Privacy (PGP), a data encryption program, is often used by investigative journalists.\textsuperscript{115}

National security services can “gather information from telecommunications systems and other data storage devices” without a warrant.\textsuperscript{116} The authorities have allegedly installed black boxes on ISP networks.\textsuperscript{117} Secret services can access and record communication transmitted via ICTs, though a warrant is required.\textsuperscript{118} There is no data on the extent to which, or how regularly, the authorities monitor ICTs. In June 2012, colleagues 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.\textsuperscript{119} 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.\textsuperscript{120} The Constitutional Court rejected the complaint, and EKINT has since stated that it plans to address the complaint to the European Court of Human Rights.\textsuperscript{121} Meanwhile, Hvg.hu filed a data request to the Ministry of Justice asking how many times the minister has provided permission for the Counter Terrorism Center to gather data secretly.\textsuperscript{122}

Privacy International found that Hungarian law enforcement agencies are connected with at least one surveillance technology company,\textsuperscript{123} and that several government agencies attended the ISS World surveillance trade shows over the years.\textsuperscript{124} Citizen Lab also reported finding a FinFisher Command & Control server in Hungary,\textsuperscript{125} though it is not clear whether the server is operated by the government or other actors.\textsuperscript{126}

\begin{footnotesize}
\footnotesize
\begin{enumerate}
\item Act XIX of 1998 on criminal proceedings, Art. 178/A, par. 1.
\item Act CXXV of 1995, Art. 56.
\item 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.
\item The complaint can be downloaded at: http://ekint.org/ekint_files/File/constitutionalcomplaint_tek.pdf.
\item "Constitutional Court: Covert surveillance based on ministerial permission des not violate the right to privacy," Eötvös Károly Institute, December 3, 2013, http://ekint.org/ekint/ekint_angol.news.page?nodeid=635.
\item For their eyes only: The commercialization of digital spying," Citizenlab.org, September 16, 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/.
\end{enumerate}
\end{footnotesize}
According to the Electronic Communications Act, electronic communications service providers are 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, caller 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 of the queries for data made by the 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.

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 of Index.hu, whose nose was broken by an extreme-right protester at an anti-government rally.

Technical attacks are common in Hungary, perpetrated primarily by non-state actors against government websites, though no major attacks were reported during the coverage period. In response to Hungary's 2010 media laws, the international hacker group Anonymous posted a video on YouTube threatening the Hungarian government with a cyberattack in August 2011. Since then, the group rewrote the new Hungarian constitution on the website of the Constitutional Court, and several government sites, including that of the National Board Against Counterfeiting and the personal website of the Minister of State for Education, were disrupted via distributed denial-of-service (DDoS) attacks in early 2012. Additionally, the website of Közgép, a construction company that frequently wins public procurements, was attacked on September 5, 2012.

127 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 electronic communications network; it does not include information society services, defined under separate legislation, which do not consist primarily in the conveyance of signals on electronic communications networks," Act C of 2003, Art. 188, par. 13.
129 Act C of 2003, Art. 92, par. 2.
131 Act C of 2003, Art. 159/A, par. 7.
135 Máté Nyusztay, ‘A rendszert támadjuk’ – Magyarország is az Anonymous célkeresztjében [‘We attack the system’ – Hungary is among the targets of Anonymous], Nol.hu, February 15, 2012, http://nol.hu/belfold/a_rendszert_tamadjuk__-magyarorszag_is_az_anonymus_celkeresztjeben.
days later, several Hungarian members of Anonymous were arrested,\textsuperscript{137} although the accused were discharged to prepare for the defense. In January 2013, the websites of Prime Minister Viktor Orbán (Miniszterelnok.hu, Orbanviktor.hu) were also hacked by Anonymous.\textsuperscript{138}

\textsuperscript{137} “Elfogták a magyar Anonymous tagjait” [Hungarian members of Anonymous were captured], Index.hu, September 8, 2012, http://index.hu/belfold/2012/09/08/elfogtak_a_magyar_anonymus_tagjait/.

Iceland

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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: 300,000

Internet Penetration 2013: 97 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: No

Bloggers/ICT Users Arrested: No

Press Freedom 2014 Status: Free

Key Developments: May 2013 – May 2014

- The proposed law to ban online pornography has not been implemented, and no changes to this legislation have been formally proposed since the change in government in 2013 (see Limits on Content).

- The crowdsourced, non-binding draft constitution has been stalled after the change in government (see Limits on Content).

- The Icelandic Modern Media Initiative, which aims to transform Iceland into a global free-speech safe haven, has progressed very slowly since its start in 2010 (see Violations of User Rights).
Introduction

Iceland has one of the highest rates of internet and social media use in the world, according to the World Economic Forum.¹ In the wake of the country’s financial collapse in 2008 when the three major banks went bankrupt, social media platforms such as Facebook were integrated into the process of creating a new crowdsourced constitution,² but the process has stalled after the change in government following the parliamentary election on April 27, 2013.³ 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. 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,⁴ though its progress has been stalled since the change in government.⁵ Similarly, there have been no new developments regarding the plan for banning pornographic content online, originally proposed by the former minister of the interior, Ögmundur Jónasson in February 2013, since the change in government.⁶

Obstacles to Access

Iceland is one of the most connected countries in the world, with the highest percentage of households in Europe with access to the internet. According to the International Telecommunication Union (ITU), Iceland had an internet penetration rate of nearly 97 percent in 2013, compared to 91 percent in 2008,⁷ with only a minimal difference in usage between the capital region and the other regions of the country.⁸ This is the highest percentage of internet users of all European countries, compared to an average internet penetration rate of 72 percent within the European Union.⁹

Iceland 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 1999.¹⁰ In 1998, broadband connections were put into operation, 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.¹¹ In 2007, the Icelandic city

---

3 Email interview with former employee at the Icelandic Media Commission, Jan 29, 2014.
4 International Modern Media Institute, https://immi.is/.
5 Email interview with former employee at the Icelandic Media Commission, Jan 29, 2014.
6 Email interview with employee from the Icelandic Ministry of the Interior, February 6, 2014.
of Seltjarnes became the first municipality in the world where every citizen has access to fiber-optic
internet service.\footnote{Idega-website, “Seltjarnes,” \url{http://www.idega.is/pages/vidskiptavinir/seltjarnarnes/?iw_language=en}}

The price of accessing the internet via computers and mobile phones is very affordable: a basic
internet subscription with 1 GB of data costs around ISK 3,990 per month (approximately US$34),
and a basic mobile phone connection with 500 Mb of data costs around ISK 590 per month
(approximately US$5),\footnote{Síminn Iceland: \url{http://www.siminn.is/english/mobile/mobile-internet/}.} while the average monthly salary is approximately ISK 560,000 (US$4,800).\footnote{Statistics Iceland, “Wages,” \url{http://bit.ly/19JQxja}}

Icelanders are frequent internet users, with 91 percent connecting to the internet daily or almost
daily. A vast majority of the population (78 percent) is connected via broadband, and a growing
number (21 percent) are connected via fiber-optics.\footnote{Post and Telecom Administration, “Statistics on the Icelandic Electronic Communications Market for the First Half of 2013,” \url{http://bit.ly/LE0us9}} According to the ITU, Iceland had a mobile phone penetration rate of 108 percent as of 2013.\footnote{International Telecommunication Union, “Mobile-cellular subscriptions,” 2013, \url{http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx}} In addition, mobile phones are widely used to
access the internet, and 58 percent of Icelanders have a mobile connection of 3G or faster, which is a
significant increase from 44 percent in 2012. In total, 63 percent of Icelanders access to the internet
professional networks, 86 percent read online news, and 90 percent use online banking. Icelandic
enterprises have the highest usage of social media in Europe (59 percent); in addition, 15 percent of
the enterprises have a blog and 19 percent use multimedia platforms to share content.\footnote{Statistics Iceland, accessed August 2014, \url{http://www.statice.is}.}

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, 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.

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 Íslands, which was privatized in 2005, and the company Skipti ehf. Of
the ISPs in Iceland, Síminn holds the largest market share (50.6 percent), followed by Vodafone (32.2
percent), Tal (9.8 percent), Hringdu (3.1 percent) and other companies comprising the remaining 4.3
percent. Regarding market share in mobile broadband, Síminn is the leading provider with almost
half of the market share (47 percent), followed by Nova (25 percent), Vodafone (24.5 percent), and
Iceland

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. In addition to the PTA, the Ministry of the Interior is responsible for legal matters relating to online content.

A new media law was established on September 1, 2011 that continued to stir debate in subsequent years. 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.

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. The commission has extensive powers to impose fines on media outlets, as well as require media outlets to register with a detailed “editorial strategy” that outlines their own set of rules for editorial independence in cooperation with the Association of Journalists or a similar entity. In 2012, all media companies had to set such rules as part of the self-regulation process, and no decisions have yet been made regarding online media by the Icelandic Media Commission. The role of the Media Commission has been widely discussed, but there have been no changes to the amendment.

Limits on Content

Access to information and online communication is free from government interference. Iceland is not a member of the European Union; however, since the country is part of the European Economic

21 Email interview with former employee at the Icelandic Media Commission, Jan 29, 2014.
Area, it has agreed to follow legislation regarding consumer protection and business law similar to other member states, which leaves the legal status of file-sharing websites such as Pirate Bay up for debate. In April 2013, the Pirate Bay website 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 to a top level domain registered in the Caribbean, even though ISNIC stated it had no intention of trying to seize the domain. In fact, the chief technology officer of ISNIC stated that even if they received a court order from the Swedish authorities, ISNIC would “legally fight attempts to use the domain name registry system to police/censor the net,” believing that such methods of combating illegal content are “ineffective, wrong and dangerous to the stability of the DNS as a whole,” highlighting Iceland’s liberal approach to regulating online content.

According to Icelandic law, the registrant is responsible for ensuring that the use of the domain is within the limits of the law. In April 2013, the Icelandic Supreme Court confirmed the Reykjavik District Court’s ruling ordering Valitor (the Icelandic partner of Visa and MasterCard) to remove the unlawful block on donations to the website for the organization WikiLeaks or face daily fines of ISK 800,000 (US$7,000). Valitor started processing payments promptly after the Supreme Court order.

Similar to other Nordic countries, ISPs in Iceland filter websites containing child pornography. The ISPs collaborate with the Icelandic Save the Children Barnaheill and participate in the International Association of Internet Hotlines (INHOPE) project. In addition, pornography in general is illegal in Iceland, although the ban is not strongly enforced. In 2013, the previous minister of the interior, Ögmundur Jónasson, proposed two new bills to the parliament in order to uphold and reinvigorate an existing law banning pornography and gambling online that is rarely enforced and vaguely worded. The ban focused on pornography that is defined as violent and degrading material, and a committee of experts was tasked with exploring how a ban on pornography could be enforced—for example, by making it illegal to pay for pornographic material with Icelandic credit cards, or by creating a national internet filter and a blacklist of websites that contain pornographic content. 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. 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.

---

26 The URL www.thepiratebay.is is automatically transferred to www.thepiratebay.xs.
30 Omar R. Valdimarsson, “WikiLeaks Sees Credit Cards Donations Return after Court Riling,” Bloomberg, May 9, 2013, http://bloom.bg/1gSOodq
32 “Banning the Sex Industry - Naked Ambition,” The Economist, April 20, 2013, http://econ.st/12q1wwM.
34 Email interview with an employee from the Icelandic Ministry of the Interior, February 6, 2014

---

377 www.freedomhouse.org
Iceland

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. Iceland has 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. A poll among politicians running in the May 2010 municipal elections showed that many considered Facebook to be the second most important medium during the election for reaching the general public in their municipalities, second only to local newspapers.

ISPs and content hosts are not held responsible for the content 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.

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. During the previous parliamentary session, Minister of the Interior Ögmundur Jónasson presented a bill to ban online gambling by prohibiting Icelandic credit card companies from processing payments to gambling websites; however, the bill was not passed. 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.

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.

Iceland has a vibrant digital sphere, and almost all traditional media, including print, radio, and television, offer versions of their content online. 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 (90 percent) are online bank users. E-governance initiatives have been successful in Iceland, and Iceland Statistics states that approximately 75 percent of the population obtained information from the websites of public authorities in 2012. In recent years, public institutions have started a migration process from proprietary software to free and open

---

Iceland

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.

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 with the constitution in accordance with an agreement reached by parliamentary parties. Four committee members were nominated by parties in government and four by parties in the opposition. The chairman was appointed by the prime minister without previous nomination. The committee is to have regard for work done in recent years, including the work of “the Constitutional Council” in 2011 and is to inform the relevant parliamentary committee on its progress. The aim is to present a bill before the next elections.

Social and online media were widely used in the recent parliamentary elections, which saw a historically large number of parties running for parliament. In particular, small parties with limited resources saw digital media as an inexpensive way to inform voters about their political agenda. During the 2013 campaign, the Icelandic Pirate Party, led by Birgitta Jónsdóttir, exclusively used online media to disseminate its platform supporting media freedom with a focus on the internet.

Violations of User Rights

Iceland has a strong tradition of protecting freedom of expression that extends to the use of the internet. Both the media law and the ambitious Icelandic Modern Media Initiative aim to enhance the use of online media.

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

---

45 Email interview with employee at the Legislative Department at the Office of the Prime Minister, March 13, 2014.
46 Interview with employee at the Icelandic Media Commission, May 17, 2013.
Iceland

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. As of 2014, the reform process of the ambitious initiative is progressing very slowly, although source protection has been implemented into law. Another bill on secrecy clauses for civil servants, lawyers, and others is being discussed in parliament. The current secrecy clauses are very opaque, and the initiative is part of the ongoing process of establishing protection for whistleblowers.

The minister of education, science and culture has appointed a committee of experts to report on online and offline challenges and propose recommendations for the promotion of freedom of expression and information. Appointed in 2012, the committee is tasked with drafting a whistleblower protection law, reviewing the articles on defamation in the penal code, and looking into source protection and communications protection. Since the change in government in 2013, however, there has been very little progress concerning the initiative.

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.

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. Since the change to the media law, there has been a decrease in libel cases.

The government does not place any restrictions on anonymous communication. No registration is required when purchasing a SIM card in Iceland.

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. 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.

49 International Modern Media Institute, https://immi.is.
50 Interview with Icelandic Member of Parliament, February 24, 2014
51 Email interview with former employee at the Icelandic Media Commission, Jan 29, 2014.
52 Interview with employee at the Icelandic Media Commission, May 17, 2013.
53 Email interview with former employee at the Icelandic Media Commission, Jan 29, 2014.
Currently, the Electronic Communications Act of 2003 implements data retention requirements mandated by Iceland’s inclusion in the European Economic Area.\textsuperscript{58} 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.\textsuperscript{59}

There have been no physical attacks against bloggers or online journalists in Iceland. In December 2013, Iceland experienced its most serious cyberattack to date, when a Turkish computer hacker cracked Vodafone’s website.\textsuperscript{60} Since June 2013, the Icelandic National CERT, operating within the Post and Telecom Administration in Iceland, has been the national center point for cyber security incidents and participates in international efforts and cooperation.\textsuperscript{61}

\textsuperscript{58} Electronic Communications Act, March 26, 2003, \url{http://bit.ly/MfiatW}
\textsuperscript{59} Icelandic Media Initiative, \url{https://immi.is/index.php/projects/immi}.
\textsuperscript{60} Ingibjörg Rósa Bjómsdóttir, “Biggest Cyber Attack in Iceland,” Grapevine, December 3, 2013, \url{http://grapevine.is/Home/ReadArticle/Biggest-Cyber-Attack-On-Iceland}.
\textsuperscript{61} Post and Telecom Administration in Iceland, \url{http://bit.ly/LXusIn}.
India

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>15</td>
<td>13</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>12</td>
<td>10</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>20</td>
<td>19</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>47</td>
<td>42</td>
</tr>
</tbody>
</table>

* 0 = most free, 100 = least free

Population: 1.28 billion
Internet Penetration 2013: 15 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- India became the third largest internet consumer base in the world in 2013, after China and the United States (see Obstacles to Access).
- The Supreme Court is assessing the constitutionality of provisions in the IT Act and secondary legislation that restrict content and criminalize speech online (see Limits on Content and Violations of User Rights).
- The Supreme Court curtailed arrests for online expression under the IT Act, though five criminal complaints were filed for social media posts (see Violations of User Rights).
- The Central Monitoring System, a mass surveillance program which enables real-time monitoring of digital communication, is being put in place without judicial oversight (see Violations of User Rights).
Introduction

The Bharatiya Janta Party (BJP) replaced the Indian National Congress-led government after a sweep- ing electoral victory in 2014, and its leadership candidate Narendra Modi was sworn in as prime minister on May 26.1 Reports of online content manipulation rose before the polls, but discourse and social media campaigning remained robust on all sides. Blocks on content, thought to disturb public order, declined in comparison to the previous coverage period.

The regulatory framework that governs the internet in India is at a pivotal moment. The Information Technology Act 2000 (IT Act), which was amended in 2008, provides a legal framework for internet use. Section 66A of the IT Act criminalizes a wide range of speech and led to several arrests for social media posts in 2012 and early 2013. However, detentions declined in the past year in the wake of negative publicity, as well as intervention from the government and Supreme Court. Several petitioners have challenged parts of the IT Act, including rules introducing potential criminal liability for intermediary companies for content posted by third parties, as unconstitutional in the Supreme Court. The court's decision in these cases will be critical to the protection of freedom of expression online in India.

Legislation and procedures to effectively protect privacy, meanwhile, remain lacking, and the scope of a privacy law currently being drafted is unclear. Allegations of procedural abuses by state officials in surveillance cases have emerged in the states of Himachal Pradesh and Gujarat, in the latter while the present prime minister was chief minister. Partly in response to these scandals, the government tightened procedures in January 2014, saying officials must issue interception orders to telecommunications providers in written form, though they still require no warrant or judicial oversight. At the same time, news reports from 2013 and 2014 indicate that the government is continuing to develop the Central Monitoring System. This ambitious nationwide surveillance program allows authorities to monitor individuals’ digital communications directly without issuing orders to service providers, written or otherwise.

Obstacles to Access

With around 200 million users2—nearly 150 million active at least once a month—India became the third largest internet consumer base in the world in 2013 after China and the United States.3 None-
theless, internet penetration remained low at an estimated 15 percent.\(^\text{4}\) India has a comparatively low broadband adoption rate, and access speeds are among the slowest in the Asia Pacific region.\(^\text{3}\)

Mobile penetration was higher at 71 percent.\(^\text{6}\) Over 230 million subscribers accessed the internet using their phones in 2013.\(^\text{7}\) Sixty-five percent of active urban internet users were mobile customers in urban areas.\(^\text{8}\) In 2013, more providers brought parity for data connection charges on 3G and earlier 2G networks.\(^\text{9}\) Bharti Airtel is the only carrier to launch 4G service so far.\(^\text{10}\) Devices remain expensive.

Information and communication technology (ICT) access was among the world’s most affordable in 2013, according to a World Economic Forum and INSEAD report, which ranked India sixth least expensive out of 144 countries for the average per-minute cost of mobile calls,\(^\text{11}\) and third for monthly fixed broadband subscriptions.\(^\text{12}\) In local terms, however, the cheapest available yearly broadband connection, INR 588 to INR 661 (\$10-$11), still represents a significant chunk of the average per capita income.\(^\text{13}\) which was estimated at INR 39,168 (\$655) for 2012 and 2013.\(^\text{14}\)

Inadequate infrastructure is an obstacle to access. India had 75 million households without access to electricity in 2013.\(^\text{15}\) In 2013, less than half of India’s internet users were from rural areas.\(^\text{16}\) Less than 19 percent of households and 20 percent of schools in rural India had computers in 2013,\(^\text{17}\) and internet access via cybercafes is declining nationwide as the number of venues shrank dramatically in the past two years. While the exact count for the coverage period is not known, an industry expert estimated the number of operational cafes declined from 75,000 in 2013 to 55,000 in 2014.\(^\text{18}\) How-


\(\text{\textsuperscript{6} International Telecommunication Union, “Mobile-cellular Telephone Subscriptions, 2000-2013.”.}\)


\(\text{\textsuperscript{8} IAMAI internet in India 2013, Internet and Mobile Association of India, p. 13, http://www.iamai.in/introductiones.aspx.}\)


\(\text{\textsuperscript{16} ‘IAMAI internet in India 2013’, Internet and Mobile Association of India, p. 2, http://www.iamai.in/introductiones.aspx.}\)


\(\text{\textsuperscript{18} Email interview with industry expert, September 2014.}\)
ever, the number of government-sponsored common service centers (CSCs) providing ICT access along with government, financial, social, and private sector services passed 90,000 in 2011 and continued to rise in 2013.\textsuperscript{19} Meanwhile, Bangalore became the first Indian city to introduce free Wi-Fi hotspots in January 2014,\textsuperscript{20} followed by Patna in February.\textsuperscript{21} Users have to authenticate their registration via mobile phones.\textsuperscript{22}

Low digital literacy and limited English also impede access. While online content is available in 17 Indian languages,\textsuperscript{23} over 100 remain unrepresented.\textsuperscript{24} Seventy-five percent of internet users in 2013 were under 35.\textsuperscript{25} The digital gender divide is also pronounced, with women consisting of only 39 percent of internet users.\textsuperscript{26} One 2013 survey found that 9 out of 10 mobile internet users in India were men.\textsuperscript{27}

Twelve submarine cables connect India to the global internet. Six are consortium owned; the rest are private.\textsuperscript{28} Cable-landing stations, where submarine cables meet the mainland, often impose hefty fees on internet service providers (ISPs); however, lower charges came into effect in 2013.\textsuperscript{29} As of 2012, there were 10 such landing stations in India, of which 5 were owned by Tata Communications and 2 by Bharti Airtel.\textsuperscript{30} News reports said India’s Competition Commission would probe the two companies for monopolizing the market in 2012, but no investigation was announced.\textsuperscript{31}

Over 80 percent of telecommunications towers are privately owned.\textsuperscript{32} 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.\(^3^3\) Bharti Infratel, a subsidiary of Bharti, is one of the largest tower infrastructure providers.\(^3^4\)

The top 10 ISPs hold almost 98 percent of the total internet subscriber base,\(^3^5\) though there were 350 ISP license holders reported in 2014.\(^3^6\) In the wired market, state-owned providers BSNL and MTNL are dominant,\(^3^7\) with BSNL holding almost 72 percent of the market as of March 2014.\(^3^8\) However, in the wireless internet market private companies have met with more success. In 2014, Bharti was the leading wireless operator, with 25 percent of the market, followed by Vodafone with 21 percent.\(^3^9\) Financial requirements are not considered a barrier to entry into the service provider market.\(^4^0\)

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.\(^4^1\) Critics said the rules were "poorly framed,"\(^4^2\) but penalties for non-compliance are not clear, and enforcement has reportedly been patchy. (CSCs are exempt, and operate under separate guidelines.\(^4^3\))

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. Within the reporting period, mobile internet access in Jammu and Kashmir was suspended for a day on July 18, 2013 after violent protests erupted in the state following unconfirmed reports that Indian border security guards had desecrated a copy of the Quran at a local religious seminary.\(^4^4\) Internet services offered by multiple cellular companies, including the 3G networks of BSNL, Airtel, and Reliance, were disconnected in Jammu and Kashmir from August 10 to August 15 during clashes.

---

40 The cost of a Unified Licence (for all services) is an entry fee of $2.44 million with a Performance Bank Guarantee of $3.6 million and Financial Bank Guarantee of $7.1 million. The license-seeker is also required to have a minimum equity of $4.07 million and minimum net-worth of $0.47 million. For individual services, the entry fee and the guarantees depend on the services. See, “Guidelines for Grant of Unified License”, January 8, 2014, http://www.dot.gov.in/licensing/unified-license.
between Hindu and Muslim communities in Kishtwar in the aftermath of the Eid festival. On February 8, 2014, the Jammu and Kashmir government partially blocked internet services for one day, after a local group proposed a commemorative strike for Afzal Guru, who was controversially convicted and executed in 2013 for conspiracy in an attack on the Indian Parliament. In March, the Press Trust of India said the Defense Ministry was seeking “interception and selective banning” of mobile internet in “terrorist hot spots” in the state.

The Ministry of Communication and Information Technology’s Department of Telecommunications (DoT) manages the overall development of the telecommunications sector, licenses internet and mobile service providers, and manages spectrum allocation. The Department of Electronics and Information Technology (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. Since 2005, the registry has functioned as an autonomous body within the not-for-profit National Internet Exchange of India.

The independent Telecom Regulatory Authority of India (TRAI) 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 licensing terms, compliance, and service quality. Its reports are published online, usually preceded by a multi-stakeholder consultation. A 2000 amendment to the act established a three-member Telecommunications Dispute Settlement and Appellate Tribunal chaired by a former senior judge. The TRAI, which criticized government departments in 2013, is perceived to be largely free of official influence.

49 See, [http://deity.gov.in/content/functions-deit](http://deity.gov.in/content/functions-deit).
51 [http://www.irinn.in/pages/static/about_us.html](http://www.irinn.in/pages/static/about_us.html).
55 The tribunal was empowered to adjudicate between licensor (DoT) and licensee; between two or more service providers; between a service provider and a group of consumers; and to hear appeals against TRAI decisions. See, Section 14, The Telecom Regulatory Authority of India Act, 1997.
India

The Supreme Court has ruled on regulation issues in the past, and said in 2012 that a “first come, first served” model of allocating spectrum was arbitrary. In October and November 2013, industry players accused the regulator of favoring incumbent 2G providers and setting auction prices too high. Lucrative 2014 auctions for two 2G spectrum bands were perceived as fair.

Limits on Content

Content blocking in the name of maintaining public order declined during the coverage period, as did over-broad copyright restrictions documented in past reports. The constitutionality of Section 69A of the IT Act, under which blocking orders are issued, is being challenged before the Supreme Court. Guidelines for intermediaries issued under the act face similar legal challenges. Reports of online content being manipulated for political purposes rose in early 2014 in anticipation of the general election, but did not significantly distort discourse or suppress mobilization.

Blocking of websites takes place under Section 69A of the IT Act, and secondary legislation passed in 2009 entitled 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” who sends the requests to the “designated officer,” and demonstrate that they are necessary or expedient under Section 69A. The designated officer chairs a committee which includes senior representatives of the law, home affairs, and information ministries, and the nodal agency for cybersecurity, the Indian Computer Emergency Response Team (CERT-IN). The designated officer issues orders approved by the committee to service providers or government agency; the committee must also notify the host of contested content of the request. In emergencies and upon written recommendations from the designated officer, the secretary of DEITY may issue blocking orders directly.

---

57 Center for Public Litigation and others v. Union of India (Writ Petition (Civil) No. 423 of 2010) with Dr. Subramaniam Swamy v. Union of India and Others (Writ Petition (Civil) No. 10 of 2011), see: http://judis.nic.in/supremecourt/imgs1.aspx?filename=39041.
60 Section 69A(1), The Information Technology Act, 2008.
61 Section 69A(3), The Information Technology Act, 2008.
63 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.
but the content must be unblocked if the designated officer does not obtain the review committee’s approval within 48 hours.65

Indian courts can order content blocks without this review process. The designated officer is required to implement the court order after submitting it to the secretary of DEITY. In reply to a Right to Information request, DEITY said the information ministry received a total of 130 court orders to block web content between February 2009 and December 2013.66

Implementation appears to depend on the technological capacity of ISPs. In the past, ISPs tampered with domain names to block content, so entire websites could be affected by a request pertaining to a single webpage.67 However, many are becoming more sophisticated. In July 2013, Citizen Lab reported 90 instances of PacketShaper technology being used in India, 53 on public networks.68 PacketShaper can delay some or all packets carrying specific information,69 so that users seeking to access it experience unreliable service and give up.70

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.”71 It is not clear how many complied.

ISPs are not legally required to inform the public of blocks and the IT Act provides for no appeal. In fact, the Blocking Rules mandate that executive blocking orders be kept confidential.72 A January 2014 transparency report issued by Verizon stated that the Indian government required the company to block access to websites, but was precluded by law from identifying how many blocking requests were received.73 Court orders can theoretically be challenged in a higher court, but internet users are not consistently notified of their implementation.74

The scale of blocking is consequently difficult to assess. In February 2014, the minister of communication and information technology told parliament that 62 URLs were blocked in 2013 through the government process under Section 69A for “hosting objectionable information” with “potential to disturb” public order.75 A news report separately said 26 URLs—many on social media—were blocked.

---

66 Reply to the RTI Application filed by Sarvjeet Singh at Centre for Communication Governance at National Law University, Delhi to the Department of Electronics and Information Technology, E-Security Division, March 25, 2014 (On record with the authors).
68 “Some Devices Wander by Mistake: Planet Blue Coat Redux”, Available as part of data set for Morgan Marquis-Boire, Collin Anderson, Jakub Dalek, Sarah McKune, and John Scott-Railton, July 9, 2013. The data set may be accessed at https://docs.google.com/spreadsheet/pub?key=0AtJqKcMmUwTkEMzMDk4VXV0em1mQWQtQ2FDeGNSVEE&output=html.
71 Rule 6(5), Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
India

on September 10, 2013 and another 82 blocked on September 18 after violence flared between Hindu and Muslim communities in the Muzaffarnagar district of Uttar Pradesh. Blocks related to public order declined compared to 2012, when a total of 362 URLs were blocked, 312 of them in a single instance in response to communal violence in the northeast, according to the minister.

Blocking based on court orders, however, increased in 2013. The minister said the government asked social networking sites to block 1,299 URLs in compliance with court orders between January 2013 and January 31, 2014, compared to 8, 21, and 352 URLs in 2010, 2011 and 2012, respectively. Separately in June 2013, news reports citing a government spokesperson said 39 websites had been ordered to be blocked for obscenity, based on a court order. Currently, there is no law against viewing pornography with the exception of creating, transmitting or browsing child pornography, though both the IT Act and the penal code prohibit the production and transmission of "obscene material."

Many limits on content remain obscure. In June 2013, observers noted some ISPs were blocking at least two image hosting websites and a political blog hosted on a United Kingdom-based service; the reason for these apparent blocks is not known.

Efforts to combat this lack of transparency are ongoing. As of May 2014, the case of Common Cause versus Union of India was pending before the Supreme Court. The petitioners challenged the constitutionality of Section 69A, citing the opaque procedure among other problems. In a separate petition, the NGO People’s Union for Civil Liberties (PUCL) called the Blocking Rules unconstitutional. That case has been joined with other pending Supreme Court petitions.

Content is also affected by takedown requests to service providers. In the first half of 2013, Google received 16 court orders to take down content and complied with 38 percent; it also received 147 requests from executive and law enforcement agencies, complying with 18 percent. Twitter’s transparency report for the period from July to December 2013 documents 8 takedown notices from India, with a 13 percent compliance rate.


78 http://164.100.47.132/LssNew/psearch/QResult15.aspx?qref=151915 ; See “Govt asks social networking sites to block 1,299 URLs”, The Mint, http://www.livemint.com/Politics/tpj/MqQ0S6h9aXaI9K/Govt-asks-social-networking-sites-to-block-1299-URLs.html.


80 Section 67, The Information Technology Act 2000.


85 The company reported 38 court orders and 122 executive orders from July to December 2012, with 53 and 30 percent compliance rates, respectively. See, Google, Google Transparency Report; Requests to Remove Content; From Governments; “July to December 2012,” January to June 2013; http://www.google.com/transparencyreport/removals/government/countries/.

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. However, Intermediaries Guidelines issued in 2011 required intermediaries to remove access to certain content within 36 hours of receiving actual knowledge of it, whether via an individual complaint or proactive screening. The range of content covered by the rules is particularly broad. In March 2013, a parliamentary standing committee recommended clearer definitions of prohibited content, expressing concern that the ambiguity could lead to censorship without due process and harassment of intermediaries.

In March 2013, DEITY clarified that intermediaries only need to acknowledge complaints within 36 hours, and are subsequently free to address them within a month. Technically the intermediary may refuse to remove the content without liability, but their decision can be challenged in court. If a judge decides that the information ought to have been taken down, the intermediary would be liable to fines or imprisonment, depending on the alleged offence, just like the individual who posted the content. Given these possible penalties, the framework incentivizes intermediaries to take down content, even in response to illegitimate complaints.

In 2011, a journalist filed a criminal complaint against 21 internet firms for hosting content he considered offensive. Some had the charges dismissed on technical grounds. In May 2013, the Ministry of Home Affairs told a Delhi court that U.S. authorities had refused to serve a legal summons to 11 U.S.-based companies in relation to this case, and the prosecution effectively stalled. Civil complaints against intermediaries are also being heard by Indian courts, including one against several internet firms filed by Islamic scholar Aijaz Arshad Qasmi in 2011.

Other petitions pending before the Supreme Court have challenged the Intermediary Guidelines. In Rajeev Chandrashekhar versus Union of India, a member of parliament called the guidelines arbitrary and overbroad. In MouthShut.com versus Union of India, a local web company argued that they force intermediaries to screen and censor online content. In PUCL versus Union of India, the

---

87 Section 79, The IT (Amendment) Act 2008; Section 72A, IT (Amendment) Act, 2008.
89 It covers content that is harassing, blasphemous, defamatory, obscene, pornographic, pedophilic, libelous, invasive of another’s privacy, hateful, racially or ethnically objectionable, disparaging, relating to or encouraging money laundering or gambling, or otherwise unlawful. See, Rule 3, Information Technology (Intermediaries Guidelines) Rules 2011.
96 W.P(C). No. 23 of 2013.
petitioners argued that the guidelines require private entities to adjudicate over content without legislative guidance, and without notifying or hearing the party affected. The PUCL also iterated that similar content is treated differently online than it would be offline. 98

Intermediaries can separately be held liable for infringing the Copyright Act 1957,99 under the law and licensing agreements.100 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 within 36 hours of receiving written notice from the copyright holder, pending a court order to remove the link.101 Rules clarifying the amendment in 2013 gave intermediaries power to assess the legitimacy of the notice from the copyright holder and refuse to comply.102 However, critics said the language was vague.103

Since 2011, courts have blocked content relating to copyright violations through broad John Doe (Ashok Kumar) orders, which can be issued preemptively and do not name a defendant.104 ISPs have occasionally implemented them to block entire websites instead of individual URLs, whether or not they were hosting pirated material.105 In 2012, the Madras High Court ruled that John Doe orders should not be used to block entire websites,106 and the incidence of such orders declined in the reporting period. A December 2013 order from the Delhi High Court asked several ISPs to block sites which illegally hosted the movie Dhoom 3 within 48 hours of receiving a written complaint from its production house, Yashraj Films, but limited implementation to specified URLs.107 In January 2014,

98 W.P(Crl) No. 199 of 2013.
99 In the Copyright Act, 1957, Section 51(a)(ii) read with Section 63 of Act the 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.
100 The guidelines and license requirements for intermediaries also prohibit the carrying of communication 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%20UL%20Agreement_0.pdf.
YouTube blocked a video spoofing Rahul Gandhi, who headed the Congress party election campaign, citing a copyright claim.\textsuperscript{108}

In general, self-censorship is not widespread. Some internet users in conflict regions may avoid addressing sensitive political or religious issues which other journalists and activists report freely. Criminal penalties on online speech in India have had a “chilling effect” on online speech.\textsuperscript{109} At the same time, outspoken blogs are widely visible and help inform the public. During the coverage period, websites accused the mainstream media of failing to investigate a December 2013 car crash involving a vehicle owned by a powerful businessman.\textsuperscript{110}

Economic forces also have the potential to influence online content. Paid news, or “advertorials,” are common in the mainstream media, ranging from unclear disclosure of paid endorsements to bribery and other kickbacks for coverage.\textsuperscript{111} In June 2013, Indian digital media website \textit{Medianama} reported this phenomenon had increased on digital platforms in the past three years.\textsuperscript{112}

Political parties are often thought to be impacting content on the internet, and major ones mobilized thousands of supporters using social networks in advance of the 2014 election.\textsuperscript{113} The then-opposition BJP acknowledged operating 100 social media campaigners, several of them paid, for posting under multiple IDs in early 2013, but denied allegations that they “flood the internet with right-wing propaganda.”\textsuperscript{114} The Congress party launched a rival online campaign later in the year but denied compensating participants.\textsuperscript{115} In November 2013, the \textit{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.\textsuperscript{116}

Other political mobilization was more positive. The Aam Aadmi Party, which contested assembly elections in New Delhi for the first time in 2013, used social media to mobilize voters extensively in
their campaign. Its website had over a million likes on Facebook, ahead of Congress and second only to the BJP. The party emerged with the second largest share of the vote and formed a government with the support of the Congress party, though it was less successful at the national stage in 2014.

The internet is increasing access to the public sphere in remote areas. 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 which 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, it has over 100,000 users that call 2,000 times a day.

Online media spurred social mobilization during the coverage period. In July 2013, the government announced plans to regulate the sale of acid in response to an online petition launched by the survivor of an acid attack signed by more than 27,000 people. In January 2014, former Supreme Court Justice A.K. Ganguly retired as chairman of the West Bengal Human Rights Commission after a lawyer published allegations of sexual harassment against him online. A powerful response from the internet community lead to an official investigation into the incident, and a Supreme Court committee began accepting sexual harassment complaints submitted by email.

After the Supreme Court’s reinstatement of the criminalization of homosexual intercourse in December 2013—previously lifted by a lower court—protests by members and supporters of the LGBTQI

community made extensive use of the internet. A “Global Day of Rage” protest four days after the verdict was largely coordinated on social media, spreading to 30 global cities.

**Violations of User Rights**

*Arrests under Section 66A of the IT Act declined during the coverage period after the Supreme Court enforced a government advisory trying to restrict its abuse. Though at least five criminal complaints regarding online content were filed, this marked an improvement over the previous reporting period. Several legal challenges regarding the constitutionality of Section 66A are pending. Two scandals regarding state officials allegedly abusing their surveillance powers emerged in the states of Gujarat and Himachal Pradesh, even as the central authorities continued to develop the Central Monitoring System, which will allow officials to retrieve content and metadata from any electronic communication in India in real time. In July 2013, Blackberry said the Indian government is now able to access encrypted emails and chats, excluding corporate communications.*

The Constitution of India grants citizens the fundamental right to freedom of speech and expression, including the right to gather information and exchange thoughts with others within and outside India. Press freedom has been read into the freedom of speech and expression. 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 offence, and the sovereignty and integrity of India. However these restrictions may only be imposed by a duly enacted law and not by executive action. The right to privacy has been read into the right to life guaranteed by Article 21 of the constitution.

The Indian Penal Code criminalizes several kinds of speech, and applies online. Individuals could be punished with a jail term ranging from two to seven years for speech that is found to be seditious, obscene, defamatory, “promoting enmity between different groups on ground of religion, race, place of birth, residence, language,” committing acts “prejudicial to maintenance of harmony,” or consisting of statements, rumors, or reports that may cause fear, alarm, disturb public tranquility, or promote enmity or ill will. Internet users are also subject to criminal punishment under the Official

---

128 Article 19(1)(a), The Constitution of India.
133 Section 124A, The Indian Penal Code, 1860.
134 Section 292 and 293 The Indian Penal Code, 1860.
135 Section 499, The Indian Penal Code, 1860.
136 Section 153A, The Indian Penal Code, 1860.
137 Section 153B, The Indian Penal Code, 1860.
138 Section 505, The Indian Penal Code, 1860.
Secrets Act for wrongful communication of information which may have an adverse effect on the sovereignty and integrity of India.\footnote{139}{Section 5, Official Secrets Act, 1923.}

The IT Act criminalizes online speech 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.\footnote{140}{Section 67, Section 67A, Section 67B The Information Technology Act, 2000.} Its infamous Section 66A criminalizes information that is grossly offensive, of menacing character, any information which is false, but causes “annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will.”

Arrests for online communication under Section 66A declined during the coverage period, while many earlier complaints were dropped or appeared to lapse. Although new complaints were filed, the longest period of detention reported in relation to a social media post was two days.

The central government and the Supreme Court tried to restrict abuse under the IT Act with mixed success. DEITY issued a January 2013 advisory restricting approval of Section 66A arrests to senior police officers.\footnote{141}{Advisory on implementation of Section 66A of the Information Technology Act, 2000, No. 11(6)/2012-CLFE, Government of India, Department of Electronics and Information Technology, January 9, 2013.} Despite this, police in Andhra Pradesh arrested local PUCL president Jaya Vindhyala in May 2013 for criticizing officials from Tamil Nadu on her personal Facebook account.\footnote{142}{“PUCL leader gets bail in Facebook post case”, The Hindu, May 14, 2013, http://www.thehindu.com/news/national/andhra-pradesh/PUCL-leader-gets-bail-in-facebook-post-case/article4715188.ece.} She was released after two days, but charges are pending.\footnote{143}{“PUCL Condemns Arrest of Jaya Vindhyala, PUCL - AP State President: PUCL Demands Release And Dropping Of Charges”, PUCL Press release, May 12, 2013, https://www.pucl.org/Topics/Media/2013/vindhayala.htm.}

On May 16, 2013, the Supreme Court directed states and territories to comply with the DEITY advisory, and subsequently intervened in two cases.\footnote{144}{Shreya Singhal v. Union of India Writ Petition (Criminal) 167 of 2012; Order dated May 16, 2013.} In August, police in Uttar Pradesh detained scholar Kanwal Bharti for four hours under Section 66A in August after he posted Facebook comments in support of a civil servant who allegedly demolished an illegal mosque.\footnote{145}{“Dalit scholar arrested for Facebook post on Durga’s suspension”, Hindustan Times, August 6, 2013, http://www.hindustantimes.com/india-news/dalit-scholar-arrested-for-facebook-post-on-durga/article1-1104208.aspx.} The Supreme Court required the Uttar Pradesh government to submit an explanation, but it has yet to respond.\footnote{146}{Shreya Dhoundial, Durga suspension: SC notice to UP govt over Dalit scholar’s arrest, August 16, 2013, http://ibnlive.in.com/news/durga-suspension-sc-notice-to-up-govt-over-dalit-scholars-arrest/414726-3.html; Shreya Singhal v. Union of India, Crim Petition No. 167/2012, Order dated August 16, 2013.}

Cases filed in 2014 involved social media comments about Narendra Modi and actor Aamir Khan’s television show. 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. There is a similar legal requirement to submit identification at cybercafes and while subscribing to internet connections.

The effective implementation of privacy rights remains a significant issue. Communication surveillance may be conducted under the Telegraph Act, as well as the IT Act, to protect defense, national security, sovereignty, friendly relations with foreign states, public order and to prevent incitement to a cognizable offence. Section 69 of the IT Act appears to add another broad category, allowing surveillance for “the investigation of any offence.”

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. These are reviewed by a committee of government officials of a certain rank, and carried out by intermediaries. A similar framework applies to the IT Act. Interception orders are not reviewed by a court, and are limited to 60 days and renewable for a maximum of 180 days. In emergencies, phone tapping may take place for up to 72 hours without this clearance, but records must be destroyed if the home secretary subsequently denies permission. Eight separate intelligence bodies are authorized to issue surveillance orders to service providers under these circumstances.

---


152 Section 5(2), Indian Telegraph Act, 1885.

153 Section 69, Information Technology Act, 2000.


160 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_nia2p74.
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, 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, including during the coverage period. 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.

Experts point out that despite these improvements, the framework is inadequate or inconsistent on key points. 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 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.” A privacy bill in draft since 2011 is still subject to internal discussion within the Department of Personnel and Training. It is unclear when it will be tabled.

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.

161 Section 69(4), Information Technology (Amendment) Act, 2008.
163 Section 69(4), Information Technology Act, 2000.
164 Section 26, Indian Telegraph Act, 1885.
172 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.
India

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. 173 “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. 174 The agreement remains effective, though various GSM operators are lobbying for the clause to be removed from the license agreement after most failed to comply. 175

Cybercafe owners are required to photograph their customers, follow instructions on how their cafes should be set up so that all computer screens are in plain sight, keep copies of client IDs and their browsing histories for one year, and forward this data to the government each month. 176

ISPs setting up cable landing stations are required to install infrastructure for surveillance and keyword scanning of all traffic passing through each gateway. 177 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; 178 and mandates prior approval from the DoT or a designated officer to install encryption equipment. 179

Since 2011, officials have sought to prevent international providers from encrypting user communications, 180 and required some, such as Nokia and Blackberry, to establish local servers subject to Indian law under threat of blocking their services. 181 In July 2013, BlackBerry confirmed their “lawful access capability” met “the standard required by the Government of India,” though business customers would be unaffected. 182 Citing a government document, the Economic Times said the interception

---


176 Rule 4, Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

177 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.

178 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.

179 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.


399
system would provide real time access to consumer data including email and web access. BlackBerry, which is based in Canada, would train five officials in the system in Ontario, according to the Times. Of the providers with BlackBerry access in India, the system was being installed by all but one, SSTL, which discontinued its BlackBerry service. Others delayed, citing pricing negotiations with the U.S.-headquartered company Verint Systems over the required software.

The Indian government also seeks user information from international web-based platforms. Google received 2,794 data requests from Indian government agencies from January to June 2014, a number that has increased every reporting period since the first in 2009; Google complied with 61 percent of the requests. Over the same period, Facebook said it had complied with 54 percent of 3,598 requests; Twitter said it had complied with 32 percent of 19 requests.

Besides retrieving data from intermediaries, the government’s own surveillance equipment is becoming more sophisticated. A Central Monitoring System (CMS) which will allow government agencies to intercept any online activities, phone calls, text messages and even social media conversations in real time by directly accessing interception equipment on intermediary premises, has caused widespread concern. Execution of the CMS has been entrusted to the DoT’s Centre for Development of Telematics. New reports differed as to when it would become operational, but at least one cited significant technical shortcomings preventing the system from coming online in mid-2013. A minister told parliament in February 2014 it is being phased in over the next three years.

The existing framework lends itself to misuse. On June 26, 2013 the Himachal Pradesh anticorruption bureau filed a case against unidentified people under sections of the Telegraph Act and the IT Act in relation to alleged surveillance abuse. The incumbent state Congress government said the previ-
ous BJP administration tapped over 1,300 phones when the Home Department had authorized only 170 taps. Targets included the political opposition and journalists.

In November 2013, investigative news websites Cobrapost and Gulail published allegations of illegal surveillance by the BJP state government of Gujarat in 2009. The sites said police, intelligence officials, and telecommunications company employees flouted procedure to monitor the communications of an architect from Karnataka for at least two months. The Gujarat government is investigating the leak of audiotapes documenting the surveillance. There were no prominent instances of physical attacks on bloggers, although there are reports of people being threatened with physical violence in response to their speech online. Activist Kavita Krishnan was harassed online by a person using the handle "@RAPIST," while journalist Sagarika Ghose was repeatedly threatened with gang rape on Twitter. The Criminal Laws Amendment Act in effect since February 2013 punishes cyber stalking of women. It penalizes monitoring of internet usage or electronic communication resulting in a fear of violence, serious alarm, or distress with fines and jail terms from one to three years.

Cyberattacks did not systematically target opposition groups or human rights activists during the coverage period, though one 2013 study ranked India as the fifth-most targeted country globally by phishing attacks. Between July and September 2013, Indian companies suffered a loss of approximately US$53 million via 3,750 such attacks, which disguise malicious software as legitimate emails. Hackers defaced tens of thousands of websites during the coverage period, a number that has grown more than five times since 2007.

---

Indonesia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>11</td>
<td>11</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>19</td>
<td>19</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>41</td>
<td>42</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 248.5 million
Internet Penetration 2013: 16 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- A Communications Ministry regulation could allow officials to block any online content they define as “negative,” without oversight (see Limits on Content).
- Charges filed under the defamation clause in the notorious Information and Electronic Transactions Law increased from 10 in 2012 to 18 in 2013 (see Violations of User Rights).
- In September 2013, the Defence Ministry reportedly spent $5.6 million on surveillance equipment from UK-based security company Gamma TSE (see Violations of User Rights).
Introduction

May 2014 saw Indonesia’s third election since the democratic transition in 1998 as 14 political parties competed for 500 legislative representative seats at the national level. In July, Jakarta Governor Joko Widodo was elected the country’s seventh president.

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. 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. Social media political campaigns soared during the coverage period of this report, and were used for the first time to forecast the election result. Major internet companies expressed their support for free and fair elections. Twitter Director of Political Advertising Peter Greenberger visited Jakarta; Facebook created an election tracker; and Google designed an election theme for its Indonesian search page. Joko Widodo sought public input on the composition of his cabinet via an online poll, attracting nearly 70,000 participants.

Awareness of the internet’s potential to mobilize around social causes increased in the past year, with more initiatives undertaken by civil society groups. However, religious intolerance is also on the rise, and the internet was frequently exploited to spread hate speech.

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. Charges filed under the defamation clause increased from 10 in 2012 to 18 in 2013.

The Ministry of Communication and Information continues to intensify its control over content, despite mounting criticism from the public. In late 2013, the ministry proposed a draft regulation which would grant officials broad power to filter and block any “negative” content on the internet, which civil society groups observed can be loosely interpreted according to the interest of the au-

---

3 The private firm Politicawave produced an election forecast based on real time social media commentary on different candidates. See http://bit.ly/1mWnYZ0.
4 See, https://www.facebook.com/FacebookIndonesia/app_576556312461482.
5 For the online survey form, see http://bit.ly/1s5Tn8H.
7 A number of civil society groups have rejected the Ministerial regulation draft. See, http://bit.ly/1bANn6n.
Indonesia

Other threats stem from warrantless interception of online data by the authorities and a lack of personal data protection.

In 2013, Indonesia hosted the Internet Governance Forum, attended by 2,632 participants from 111 countries. Its success was partly attributed to the major role played by civil society organizations in encouraging the government to adopt a multistakeholder approach to internet governance, both in preparing the event and as a core principle for future policy making, underscored by the adoption of an internet governance declaration.9

Obstacles to Access

Internet penetration continued to increase over the past year, though precise figures differed. The International Telecommunication Union cited 16 percent in 2013, up from 13 percent in 2012.10 The Indonesia ISPs Association, known as APJII, reported penetration at 28 percent.11

Mobile penetration reached 121 percent in 2013.12 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.13 Prepaid internet packages for smartphones range from $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.

Despite this, 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.15 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.16 In May 2013, a Moluccan...

Ring cable system was launched to connect Papua and other parts of eastern Indonesia with the existing broadband network. 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. In Papua, less than 40 percent of the population owned a mobile phone in 2013, compared to 97 percent in Jakarta. A national 2012 survey put e-literacy in underdeveloped provinces such as Papua and Mollucan far lower than the national average.

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. A 2012 ICT white paper set out to eliminate the digital divide by connecting 33,000 villages, though that target had yet to be reached by the end of 2013.

The infrastructure project was halted during the coverage period of this report over corruption allegations. In July 2013, the Attorney General’s Office opened a criminal investigation naming government officials and private sector businessmen as suspects. It is not clear when the case file will be submitted for trial.

There are about 300 ISPs providers 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 Telkomsel, with a market share of 60 percent, and PT Indosat with 21 percent. A third, XL-Axiata, accounted for 19 percent.

Despite some individual allegiances to officials, Indonesian ISPs are a close-knit community thanks to the APJII, which was founded in 1996. In 1997, tired of routing local traffic through expensive and inefficient international channels—and wary of a government-led solution—they independently created the Indonesia Internet Exchange to allow member ISPs to interconnect domestically and to
increase domestic traffic. Although the peering was initially limited to member ISPs, since 2011 the service has been extended to non-members. APJII also engages the government on behalf of providers regarding censorship, legal, and regulatory issues in ways that freedom of expression experts view as largely constructive.

In January 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 ($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.

In July 2013, however, 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.

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 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. However, the body has been seen as toothless. It is not equipped with executive power, but can only make recommendations, and as a result fails to intervene in relevant fraud or corruption cases.

---

27 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.
30 See, http://bit.ly/1nYlxSW. Twelve ISPs were closed down by the government in 2012 after failing to produce the fee.
Limits on Content

At the end of 2013, the MCI proposed a draft regulation on negative content supposedly targeting pornography. The draft spurred criticism from rights groups, concerned that the regulation will be used to expand the existing practice of filtering and blocking of online content without adequate oversight or an avenue of appeal. In April 2014, the Press Council formally objected to the draft in a letter to the MCI. Claiming to have been working on it for more than two years, however, the ministry appeared resistant to consultation on the content of the regulation during the coverage period of this report.

The MCI restricts content posted online by blocking and filtering access to certain websites. This power 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 of the article 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.

A ministerial regulation drafted in late 2013 threatened to introduce further blocks on any negative content, with the scope of “negative” to be determined by the MCI. Though introduced as a countermeasure to online pornography, the draft’s definitions were broader than those already outlined by the pornography law. If passed, it could result in limitations on freedom of expression far more extensive than those allowed under international standards. In addition, the regulation could allow nonstate entities to practice filtering and blocking independently. It lacks transparent procedures for complaints or remedies for the victims in the case of overblocking, and contains no requirement for judicial oversight. As of May 2014, the regulation was still in draft form.

Existing blocks predominantly target pornographic sites, sexual content, or gambling. The ministry is not known to systematically filter political content or antigovernment criticism, though other broad restrictions are in place. Encryption and circumvention tools are blocked, though in practice some remain accessible. As of October 2013, they were “heavily filtered on Telkmonet’s IGF network while generally available on the other two networks.” Sites that promote terrorism and file-sharing are also subject to restrictions. In 2012, the APJII mooted banning all websites that allow illegal downloads, but the restriction never emerged.

In 2010, the MCI introduced “Trust+,” a filtering application containing a database managed directly by the ministerial office, which is continuously updated. According to the annual MCI report, 9,894 sites were added to the total Trust+ list of 800,048 sites in 2013. People can also request websites

---

33 See, Law No. 11/2008, Article 40.
34 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.
be added via a public email address. 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+” or an independent list. This creates uncertainty for users seeking redress when content is wrongful blocked.

Since filtering relies on keywords, blocks can be overly broad. Some minority voices, particularly LBGTI groups, suffer from arbitrary filtering. In April 2013, the LBGTI 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+” 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. A 2013 news report said it had blocked 600 fraudulent online stores. Its database included 811,190 sites by January 2014. Nawala provides a form for website owners subject to accidental blocking, though how it processes complaints.

Administrative requests to delete or take down content are less common. From January to June 2013, the government requested that Google remove six YouTube videos based on copyright complaints, but none were removed. Overall, the government flagged 49 items for Google to remove, of which 40 involved alleged religious offenses.

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 after the government regulator warned that the firm’s market access could be restricted if it failed to comply.

40 According to tests conducted by OpenNet Initiative in 2009 and 2010, three out of seven major ISPs in Indonesia filtered content through HTTP proxy blocking; the tests did not reveal whether or not they applied Trust+. See, OpenNet Initiative, “Indonesia,” August 9, 2012, https://opennet.net/research/profiles/indonesia.
No self-censorship among journalists or internet users due to political pressure was reported during the coverage period of this report. While interference from state agencies has declined significantly compared to past years, social pressure often leads to self-censorship among journalists, and occasionally manifests online in relation to religion, sensitive political corruption charges, or potential defamation.46 Religious hardliners threatened media practitioners during the coverage period. In June 2013, the Islamic Defender Front warned one media owner for its coverage, which was perceived to discredit the organization, and demonstrated against another company for broadcasting a Miss World contest.47

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 rumors 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.48 Social media pages have also been used by religious extremists. In June 2013, an expert told the Associated Press that 50 to 100 militants had been recruited directly through Facebook in the past two years.49

The internet has also strengthened grassroots mobilization. The Jalin Merapi network offered relief to communities affected by the Merapi volcano eruption in Central Java in 2010. Initiated by community radio stations, the response used the Twitter account @jalinmerapi to coordinate meals for 30,000 people in less than four hours, while the government was slow to react.50 The Indonesia Breastfeeding Mothers Association (@aimi_asi) 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,51 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.52

In a rare response to criminal proceedings on a defamation case in 2013, many netizens mobilized support under the hashtag #savebenhan after Benny Handoko was arrested for a tweet accusing a former legislator of corruption. Public pressure contributed to his release from pre-trial detention.

46 Interviews with Abdul Manan, senior journalist from Tempo newspaper, and Nezar Patria, managing editor of Viva News, 2013. There is no official data for threats against journalists, but cases of retaliation for news coverage are common. See, http://www.beritametro.co.id/jawa-timur/kantor-redaksi-diserbu-massa
51 See, http://indonesiaberkebun.org/about/.
Violation of User Rights

While 18 criminal defamation charges were filed in 2013, the only sentence related to online content passed during the coverage period was the one year of probation handed down to Benny Handoko in relation to a tweet about corruption. In September 2013, the Defence Ministry reportedly spent $5.6 million on surveillance equipment from UK-based security company Gamma TSE.

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.\(^{53}\) The constitution also includes the right to privacy and the right to gain information and communicate freely.\(^{54}\) These rights are further protected by various laws and regulations.\(^{55}\) Indonesia also ratified the ICCPR in 2005.\(^{56}\)

Other laws passed since then have infringed on user rights, despite legal experts’ opinions that they conflict with the constitution.\(^{57}\) 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.\(^{58}\)

Provisions of the 2008 ITE Law have been used repeatedly to prosecute Indonesians for online expression. 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.\(^{59}\) Financial penalties show an even more surprising discrepancy. While the ITE law allows for fines of up to IDR one billion ($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.\(^{60}\)

In the five years since the ITE law was enacted, 35 people have been criminally prosecuted for online defamation. Cases increased from 10 in 2012 to 18 in 2013, according to Indonesian NGO ELSAM.\(^{61}\) Prosecution begins when the affected politician or official files a case with police. Defamation cases

---

53 Constitution of 1945, Article 28E(3).
54 Constitution of 1945, Articles 28F and 28G(1).
56 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.
60 “Kitab Undang-Undang Hukum Pidana” [Criminal Law], available at Universitas Sam Ratulangi law faculty, http://hukum.unsrat.ac.id/uuj/kuhpidana.htm#b2_16.
61 For a detailed list of ITE law cases through 2014, see ELSAM, http://www.elsam.or.id/downloads/104168_KASUS_ITE_per_Maret_2014.pdf. No official data on the number of defamation cases is available. Safenet, a network of South East Asia bloggers and online activists reported 21 criminal cases related to online expression.
increasingly stem from social media status updates. On February 17, 2014, Fadlin Akbar, the son of a former mayor of Tangerang city, reported journalist Deni Irawan of the *Sindo* newspaper to police for allegedly defaming him in his Blackberry Messenger (BBM) status. Fadlin withdrew the report after the journalist publicly apologized. In August 2013, Kadir Khalid, a member of a local legislative body in Makassar, South Sulawesi, reported a man to police when his BBM status accused Nurdin Khalid, his brother and fellow politician, of corruption. The man, M. Arsyad, was detained for 93 days while awaiting trial, and released after the court acquitted him on May 25, 2014.

In one high-profile case, a South Jakarta district court sentenced Benny Handoko to a year on probation on February 7, 2014 for comments posted on Twitter in December 2012 accusing a former Social Welfare Party legislative member of corruption in relation to a scandalous bailout of Centurion Bank. His detention on September 5, 2013 spurred significant criticism on social media, since pre-trial detention should only apply in cases where there is substantial evidence that a suspect will destroy evidence, repeat a criminal act, or abscond. Handoko was released after one day. The prosecutor’s office challenged the district court’s decision and is appealing the sentence.

Observing the adverse impact of the application of the ITE law, particularly the disproportional criminal sanctions for defamation, civil society groups have called for it to be amended. However, the government has yet to propose a draft amendment for deliberation.

A 2011 State Intelligence Law introduced penalties of up to ten years’ imprisonment and fines of over $10,000 for revealing or disseminating “state secrets,” a term which is vaguely defined in the legislation. 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.

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 ignored in practice since at least 2011. 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. When they developed this in Singapore instead of Indonesia, the government threatened to introduce a regulation requiring telecommunications companies to build local data centers, though this has yet to materialize.

---

Indonesia

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.69 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.70 In addition, the legal framework lacks judicial or parliament oversight, and does not provide a remedy for possible abuse.

In September 2013, the Defence Ministry reportedly spent $5.6 million on equipment for surveillance, including encryption, decryption, and data communication surveillance tools, from U.K.-based security company Gamma TSE.71 Given Indonesia’s weak privacy protections, this procurement has raised concerns that more user rights may be infringed. These increased in February 2014 when news reports said Jakarta Governor and presidential candidate Joko Widodo’s home and office had been wiretapped.72 It was not clear who was responsible and there are no reports on whether the police carried out a criminal investigation.

In November 2013, documents leaked by former U.S. National Security Agency (NSA) contractor Edward Snowden revealed that the NSA and the Australian Signal Directorate (ASD) were monitoring mobile phones belonging to President Yudhoyono and his political associates.73 The disclosure prompted widespread anger, and the president and parliament threatened to suspend bilateral cooperation with Australia. The ministry also investigated the alleged involvement of two domestic ISPs in the surveillance, though no criminal charges have been reported. 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.74

Cyberwarfare between anonymous hacking groups in both countries escalated following these reports. The group Indonesia Security Down hacked websites run by the Australian government, spurring a counter attack from Australian hackers who uploaded stolen data to the web, including details of frequent flyers with flagship airline Garuda, information on central Java’s Adi Sumarmo Airport, and a Ministry of Education online database.75 Politically motivated cyberattacks against civil society groups have not been reported in Indonesia.

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

72 See, http://bit.ly/1lauDZg
unannounced searches of cybercafes, which are perceived as promoting immoral conduct;\textsuperscript{76} no incidents were documented during the coverage period.


## Iran

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>32</td>
<td>31</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>37</td>
<td>36</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>91</td>
<td>89</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

| Population:                      | 76.5 million |
| Internet Penetration 2013:       | 31 percent   |
| Social Media/ICT Apps Blocked:   | Yes          |
| Political/Social Content Blocked:| Yes          |
| Bloggers/ICT Users Arrested:     | Yes          |
| Press Freedom 2014 Status:       | Not Free     |

### Key Developments: May 2013 – May 2014

- Iran ranked 156 out of 192 countries for internet speed and has the lowest average peak connection speed in the world. The new government promised to increase the average speed two-fold by the next year, and eight-fold by the end of President Rouhani’s first term (see Obstacles to Access).

- Although the new administration has embraced social media, major platforms like Twitter and Facebook remain blocked and inaccessible to Iranian citizens (see Limits on Content).

- While the election of Rouhani has resulted in enthusiasm, including a mild decrease in self-censorship online, significant constraints on speech and access to information remain present. Censorship was particularly heavy in the lead-up to the June 2013 presidential election, and Sunni-linked sites have come under target as regional sectarian tensions continue to enflame (see Limits on Content).

- Six Iranians were arrested for producing and appearing in a YouTube video entitled “Happy in Tehran,” featuring men and women dancing together, without headscarves, in a similar fashion to hundreds of homemade videos from around the world that mimic the “Happy” music video by popular American musician Pharrell Williams (see Violations of User Rights).

- Although there were no documented cases of deaths this year, Iranians continue to be receive lengthy prison terms for their online activities. Tech bloggers in Kerman, contributors to a Sufi website, and Facebook page administrators were jailed for up to 20 years (see Violations of User Rights).
Iran

Introduction

On June 14, 2013, Iranians took to the polls to elect a new president for the first time since the deeply flawed presidential elections of 2009, which led to large-scale protests and a violent crackdown on supporters of the opposition “Green Movement.” With an eye on preventing a repeat of 2009, authorities waged an aggressive campaign of filtering websites, blogs, and even text messages that expressed support of certain political candidates. In the week leading up to the vote, the disruption of services reached its peak. Encrypted traffic was throttled to five percent of normal speeds or less, and the authorities used a “white list” to block all international connections that were not pre-approved. Because of this, most online tools that allow users to circumvention censorship and communicate anonymously were blocked or dysfunctional. A large number of Iranian activists and journalists were targeted by sophisticated malware attacks or smear campaigns on social media.

The election result surprised many observers with Hassan Rouhani, commonly seen as the moderate candidate, winning the election. One day after the results, online restrictions reverted back to pre-election levels. Upon assuming office, several actions by the Rouhani administration were interpreted by observers as a sign of a potential liberalization of internet policy. Despite the fact that Facebook and Twitter are blocked, the vast majority of Rouhani’s cabinet ministers have opened up social media accounts. On September 17, Facebook and Twitter were also temporary unblocked, ostensibly due to a technical error. However, nearly one year after the beginning of Rouhani’s presidency, no major changes to the situation have occurred. Widespread filtering and the blocking of social media tools and mobile apps remain in place. The implementation of the National Information Network, considered a priority of the Rouhani government, has been sped up. In addition, a significant number of Iranian bloggers, techies, and activists have been arrested for their online activities and received heavy prison sentences. Several tech bloggers and digital activists were arrested in the city of Kerman for alleged links to “espionage networks” and “foreign media,” apparently relating to journalism training programs offered by the British Broadcasting Corporation (BBC). Meanwhile, seven contributors to Sufi website Majzooban Nor were convicted of producing antigovernment propaganda, insulting the Supreme Leader, and endangering national security, with the heaviest sentence 10 years. Finally, eight individuals were sentenced as much as 20 years of jail time for “blasphemous” or “anti-regime” Facebook posts.

The internet was first introduced in Iran during the 1990s to support technological and scientific progress in an economy that had been badly damaged by eight years of war with Iraq. Until 2000, the private sector was the main driver of internet development. This changed under the government of the reformist President Mohammad Khatami (1997–2005), when the authorities invested heavily in expanding the internet infrastructure, but also began to clamp down on free expression online. Meanwhile, Supreme Leader Ali Hosseini Khamenei first asserted control over the internet through a May 2001 decree that centralized service providers’ connections to the international internet. 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. Despite all of these limitations, the internet remains the only viable means for Iranian citizens and dissenters to obtain news and

1 Though confirmed details of the National Information Network remain sketchy, objectives include the mandatory registration of internet protocol (IP) addresses, the moving of government-approved websites to servers based inside the country, and the launching of Iranian equivalents of major online services like email, social-networking sites, and search engines. These measures will restrict online anonymity, increase monitoring capabilities, and allow Iranian authorities to control access to particular international communication flows during periods of political unrest without the need to shut down all domestic services.
organize themselves. Traditional media outlets are tightly controlled by the authorities, and satellite broadcasting from outside Iran is subjected to heavy terrestrial jamming.

In general, internet policy remains a contested space in Iran, with authorities continuing to favor a ‘militarized’ approach, viewing the internet as a threat to national security. Such discourse has been criticized by many regime insiders, including Ali Akbar Hashemi Rafsanjani, former Iranian president and current chairman of the Expediency Discernment Council, who stated that using security concerns to obstruct the development of the information and communications technology (ICT) industry is irrational and futile. Such comments, in addition the Rouhani administration’s failure to lift online restrictions, confirms that the government has little control over the country’s internet policy. Instead, like many other aspects of policymaking in Iran, the sector is beholden to a complex web of interests but ultimately sanctioned by the Supreme Leader, Ali Khamenei.

**Obstacles to 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 a report released by the newly appointed Minister of ICT, internet penetration rate is at 43 percent, with 30 million total users. In addition, the report indicates that there are 4.1 million high speed internet access ports in operation. This contradicts a June 2013 report by the National Internet Development Management Centre (MATMA), which put the penetration rate at 61.1 percent.

In contrast, the International Telecommunication Union (ITU) estimated the number of internet users in Iran at 31 percent for 2013. Citing the Iranian Information Technology Organization as its source, the ITU also said there are only 5.62 fixed-broadband subscriptions per every 100 inhabitants.

Internet speeds are incredibly slow in Iran, ranked 156 out of 192 countries tracked by OOKLA, which performs broadband speed testing globally. Iran had the lowest global average peak connection speed at the end of the first quarter of 2014, according to Akamai. The average peak connection speed was 6 Mbps, but it was up 87 percent from the previous year, which highlights the significant limitations imposed on the internet in Iran in the period leading up to the presidential election.

Mehdi Akhavan Behabadi, the former secretary of the Supreme Council of Cyberspace, said in an interview that the main issue affecting the speed and cost of access is the practice of price inflation by the Telecommunication Infrastructure Company (TIC), which buys access at 1Mbps for US$ 15 and resells to ISPs for over US$ 100. He decried the lack of competition due to the TIC’s

---

2 “Heavy criticism of Internet filtering in Iran by Hashemi Rafsanjani”, Khabar New, accessed February 10, 2014 [http://www.khabarnew.ir/NSite/FullStory/News/?Serv=0&Id=34649&Sgr=0](http://www.khabarnew.ir/NSite/FullStory/News/?Serv=0&Id=34649&Sgr=0).


monopoly as a bandwidth provider, and called for privatization of the sector. The Ministry of ICT has further expanded its monopoly over internet infrastructure by banning the importation of any telecommunications equipment that is not authorized by the ministry. Such regulation will make it even harder for the private entities to compete with a state-backed entity.

Apart from market forces, political factors contribute to the low speeds in Iran. The former Minister of ICT under the Ahmadinejad administration confirmed that the government slowed internet speeds in the days prior to the presidential election as part of “security measures taken to preserve calm in the country during the election period.” Prior to this announcement, authorities had never acknowledged a connection between an election and a decrease in internet speed.

The new ICT minister, Mahmood Vaezi, has announced that average internet speeds will increase two-fold in the next year, and eight-fold by the end of President Rouhani’s first term. With regards to ICTs, he has also promised to restore the status quo that existed prior to 2005, when Ahmadinejad took office. Vaezi has stated he believes that access to ICTs has hardly expanded since 2005, and in some cases, the industry has actually shrunk.

However, it is unclear whether this promise to increase internet speeds under Rouhani is related to access to the global internet, or solely the National Information Network (NIN), which would only result in faster access to sites hosted within Iran. Rouhani has emphasized the importance of the NIN and has urged the different bodies under his control to expedite its implementation. Officials from the government have even reached out to their Chinese counterparts to enlist their help with its completion. While the NIN was being implemented, Iran fell short of its target to reach a bandwidth capacity of 500 Gbps by March 2014; it was below 80 Gbps in February. According to Vaezi, accessing information hosted on the NIN will be fast and cheap, while websites hosted outside the country will be available at slower speeds.

Through a mix of coercion and economic incentives, authorities have been pushing popular Farsi-language websites operated from inside the country to use domestic hosting services on the NIN. Iran has also been trying to launch national versions of popular online services, such as email and search engines. Despite a large investment, these national services have largely failed to attract Iranian users.

Similar to the internet penetration rate, statistics provided by various Iranian officials on mobile phone penetration are contradictory. Ali Kargozar, director of the Fixed Communication Company of Iran (FCI), stated that 100 million SIM cards are active in Iran, a penetration rate of 110 percent.

---

8 “Mehdi Akhavan Behabadi Criticizes Iran’s Telecommunication Infrastructure Company for its Pricing Model”
9 “Importation of Telecommunication equipment is only allowed with the Ministry of ICT permit”, Young Journalist Club, accessed February 11, 2014 http://goo.gl/fsp0Yh.
11 “Speed of Internet will increase 8 fold”, ISNA< accessed July 21, 2014 http://goo.gl/AheEOY.
Vaezi put mobile phone penetration at 79 percent.\(^{15}\) Regardless, it is clear that Iran’s mobile telephone sector continues to grow. According to the ITU, Iran had a mobile phone penetration rate of 84.25 percent, up from 76.1 in 2012.\(^{16}\) The penetration of smartphones and mobile internet is also increasing. According to Mahmood Liyaei, an adviser to the Ministry of ICT, Iran has 4 million Android users, accounting for 10 percent of total internet traffic. Cafe Bazaar, a locally developed Android app store, is itself responsible for 2 percent of traffic. According to other statements by Liyaei, mobile technology represents an annual market of around US$ 4 billion in Iran.

However, the telecommunications industry in Iran is tightly controlled by the government or related entities. In recent years, the role of the Islamic Revolutionary Guards Corps (IRGC)—a politically important branch of the security forces that also controls large sections of the economy—in the ICT sector has notably increased.\(^{17}\) 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. The Data and Communication Company (DCC), which operates under the TCI, retains a monopoly on internet traffic flowing in and out of Iran. 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 amongst its management. The third operator, RighTel, was launched in early 2011. It, too, is a government-owned entity.

The pre-election period in May 2013 brought about increased obstacles to access, particularly for users seeking to use circumvention tools or encryption. For example, encrypted traffic was throttled to one to five percent of normal speeds and the authorities used a “white list” to block all international connections that were not pre-approved. As such, most virtual private networks (VPNs) were also blocked.

Cybercafes are under the close scrutiny of the officials. These provided 22 percent of all Iranian users with access in 2012. Given their popularity, authorities have been attempting to control them since around 2006, through policies such as segregating business hours for men and women. In July 2013, police inspected 353 cybercafes in Tehran and closed down 67 for “violating regulations and offering illegal services harm youth and their families.”\(^{18}\)

There is no independent regulatory body for ICTs in Iran. The Communications Regulatory Authority (CRA) is responsible for telecommunications licensing. It is part of the ICT Ministry and its head is appointed by the minister.\(^{19}\) In March 2012, the broader decision-making process related to ICTs underwent a change, when Iran’s Supreme Leader Khamenei issued a decree establishing the Supreme Council on Cyberspace (SCC). The SCC is intended to provide a centralized focal point for

---


policy-making and regulation of Iran’s virtual space, effectively removing such authority from the executive, legislative, and judiciary branches of the government and bringing it under Khamenei’s direct control. Observers believe this reflected Khamenei’s dwindling trust in President Ahmadinejad and his hesitation to leave such an important area of policy under the president’s authority.

**Limits on Content**

The Iranian authorities continued to restrict access to tens of thousands of websites in 2014, particularly those of international news sources, the opposition, ethnic and religious minorities, and human rights groups. According to a member of the Committee to Determine Instances of the Criminal Contents (CDICC), an average of 1,500 websites with content considered anti-Islamic are filtered every month. While censorship remains stable, the results of the presidential election raised expectations that Rouhani would ease restrictions on online speech, resulting in a mild improvement in self-censorship. However, this enthusiasm may prove short-lived as harassment, detentions, and prosecution of internet users continues.

The regional tension between the Shiite and Sunni branches of Islam also manifests itself in the filtering of websites. The official website of Molavi Abdul Hamid, a prominent spiritual leader of Iran’s Sunni community, was blocked without any explanation. Mashregh News, a website closely aligned with the IRGC, published an article strongly criticizing the availability of a Persian-language version of the Saudi-backed *Asharq Al Awsat* newspaper online in Iran. Abdolsamad Khoramabadi, the head of CDICC, stated his agreement with the article and the site was subsequently blocked.

In the period leading up to the presidential election in June 2013, a large number of websites linked to reformists were blocked. For example, Moj11.ir, an online campaign to support Khatami in the election became unavailable shortly after launch. SalamKhatami.com, a reformist site launched to petition Khatami to participate in the elections was blocked after eight days. Reforms.ir, a reformist news site covering the election, was also blocked. Campaign sites and personal blogs supportive of then-president Ahmadinejad and candidate Esfandiar Rahim Mashaei hosted on Iranian-owned platforms were also subjected to blocking or removal.

A number of the campaign websites with the aim of keeping Iranian officials accountable were also blocked. Rouhani Meter, a website monitoring the performance of President Rouhani over the first 100 days of his administration, was blocked on August 28. Shahrdare Ma (Our Mayor) was also blocked without explanation when the website sought to gauge public opinion concerning the performance of Mohammad Bagher Ghalibaf, Mayor of Tehran. After the website was blocked, it was completely shut down and the account was suspended.

A number of popular news websites operating inside Iran were also blocked. After publishing a news story in which Ahmadinejad claimed the 2009 election was rigged, *Baztab-e Emrooz* was blocked and managing director Ali Ghazali was arrested for ‘disturbing public opinion.’ (See “Violations of

---


Iran

User Rights.") "Eghtesad Press" (Economy Press) was also blocked and shut down under order from the District Court of Area 28 in Tehran. The website had published an article accusing the head of Iran’s Securities and Exchange Organization (SEO) of corruption. "Entekhab," a popular news website based inside Iran, has been inaccessible since February 1, 2014 as a result of a complaint by the Tehran public prosecutor and a closure order issued by the Tehran media court. "Entekhab" editor Mostafa Faghihi told the government news agency Irna that the site was blocked for publishing a letter in which a university academic, Sadeq Zibakalam, criticized Iran’s nuclear policy as well as other sensitive issues such as public health and education. The website was unblocked after removing the letter and the associated user comments.

However, as part of Rouhani’s larger policy of normalizing foreign relations and improving the international image of Iran, the website of CNN was unblocked on September 28, 2013, allowing users to access its content without the use of circumvention software. The CDICC had filtered the site, along with Reuters and BBC News, in the wake of the disputed 2009 presidential elections. Of the three news sites, the BBC is the only website that remains inaccessible in Iran. The CDICC did not comment on the move to unblock CNN.

Major international social media tools, such as Facebook, YouTube, Twitter, and Flickr, remained blocked, though the presence of officials in the Rouhani administration on Facebook and Twitter led to speculation that access to these platforms may be restored. However, when the head of the CDICC spoke on the matter, he described Facebook as a project of the CIA in an attempt to collect data from individuals around the world. Khoramabadi also described Mark Zuckerberg, founder of Facebook, as a "leading Zionist," citing an occasion when Israeli President Shimon Peres described Facebook as a powerful tool for the advancement of Zionism. He later announced that Facebook will not be unblocked, as the site contains a great deal of criminal content which cannot be separated from the legal content.

The online restrictions were not limited to political and economic content. Persian language music blogs, dating sites, digital security information, and movie download hubs were subject to increased filtering and content takedown orders. Popular international music streaming services like Pandora and Grooveshark have also been blocked.

The Iranian government has blocked access to two of Iran’s most popular instant messaging and communication services. WeChat, a free voice and text messaging application developed in China, was blocked on December 19, 2013 after members of parliament and officials from Iran’s Cyber Police voiced concerns over its use among Iranian youth. Viber was briefly disabled on January 2, 2014. Cryptocat, a tool popular with human rights activists and journalists that allows secure and encrypted chat, was also blocked, demonstrating that the Iranian authorities are concerned with the popularity of communication channels that they cannot easily monitor. According to the CDICC, the committee is also considering blocking other communication platforms such as Tango, WhatsApp, and Coco as "these foreign services gather data from Iranian users to be analyzed by foreign intelligence services." All remained unblocked in May 2014.

Iran

Iranian authorities 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.

Aside from filtering, the regime 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 Computer 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 shutting of news websites hosted on platforms inside Iran, under orders from government officials. The CCL also specifies violations 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.28

In an effort to show that content filtering is based on a legal framework, institutions to oversee internet filtering have been created. The Committee in Charge of Determining Unauthorized Websites is empowered to identify sites that carry forbidden content and report that information to the TCI and other major ISPs for blocking. The committee is headed by the prosecutor general and other 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 nontransparent. 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.29 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 complaints.30 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.

In protest against the arbitrary filtering process in Iran, over 100 media activists wrote a statement objecting to “an increase in the number of confrontations outside of the standard realm of regulations in dealing with cyberspace issues.” While complaints about censorship have typically come from reformist and independent media, these activists are said to be involved in managing semiofficial news agencies and conservative websites, which faced increased censorship in the period leading up to the presidential election in 2013. According to the statement, over the course of the past year, an “unrelated government body” has been contacting official news agencies and asking them to “either remove specific text from their website or risk filtering.” The body appears to

---

be CDICC. Critics say this committee does not have the jurisdiction to deal directly with websites and news agencies that are licensed by the Press Supervisory Board.\(^{31}\)

Internet traffic over cell phones is subjected to a similar level of restrictions as fixed-line connections. 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). The content of SMS is also subjected 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 “Mashaie” were blocked, referring to Esfandiar Rahim Mashaei, the presidential candidate supported by Ahmadinejad. Texts containing political slogans related to Mashaie and Ahmadinejad had also been blocked in the past.

Currently there is no legal framework for filtering of SMS content. However, in June 2013 the director of the SCC 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.\(^{32}\) The CRA has 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.\(^{33}\)

Self-censorship is extensive, particularly on political matters. The 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. The change, however, has been more in terms of perception. 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.

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. 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.

The Iranian government has intensified its fight against the use of circumvention tools. The use of such tools is considered to be 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.

Due to the ongoing blockage of Facebook and Twitter, opposition campaigning on Persian social media is limited in reach and scope. However, all candidates maintained an active presence on social media during the presidential election, either through official or unofficial accounts linked to their campaigns. Facebook, Twitter, and Instagram accounts linked to President Rouhani have a large following.

On May 3, a London-based Iranian journalist created a Facebook page entitled “Stealthy Freedoms of Iranian Women” in order to encourage women to post photos of themselves without a hijab or headscarf. The site gained over 170,000 followers within two weeks and as of mid-2014 had over 600,000. Hundreds of women have posted photos to the site, defying national laws that require the hijab and risking punishment. Masih Alinejad, the founder of the page, was accused by Iran’s semi-official news agency of promoting promiscuity and working with the enemy.

Violations of User Rights

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 caught the ire of authorities. A group of tech bloggers in the city of Kerman were sentenced up to 11 years for alleged links with foreign organizations, while seven contributors to a Sufi website were also jailed for lengthy terms. Even if access to social media is restricted in the country, eight individuals were sentenced to jail for 7 to 20 years related to Facebook posts deemed as blasphemous or against the regime. Harassment and surveillance are rampant, particularly for those who are critical of the authorities or belonging to ethnic and religious minorities. The recent wave of arrests and sentences are considered to be part

---

36 “Iran to crack down in web censor-beating software”, AFP, accessed June 24, 2013, https://www.google.com/hostednews/afp/article/ALeqM5jIFi-LdqBsdtri7mRYmCMT1SGICCA?docId=CNG.f710a666e11dc52f64c985918d1bac1.1741.
37 See his Facebook page (over 120,000 followers) at https://www.facebook.com/Pres.Rouhani, Twitter account (250,000 followers) at https://twitter.com/HassanRouhani, and Instagram account (60,000 followers) at http://instagram.com/hrouhani.
38 See https://www.facebook.com/StealthyFreedom.
of the reaction of the hardliners within the Iranian establishment to President Rouhani’s attempts to open up cyberspace and the media. The IRGC in particular are known to be fiercely resistant to any liberalization in these areas.

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.\(^{41}\) 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.”\(^{42}\) 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.

Dozens of Iranians were arrested over the coverage period. On December 3, 2013, officials from the IRGC arrested 16 digital activists in the southern province of Kerman, including eight staff members from the gadget review site Narenji.ir or its sister sites: Aliasghar Honarmand (Narenji’s founder), Abbas Vahedi, Hossein Nozari, Reza Nozari, Amir Sadeghpour, Mehdi Faryabi, Ehsan Paknejad, and Malieh Nakhei. Referencing their apparent links to the BBC and BBC Persian, they were accused of being in contact with “enemy media” and “running a number of projects and plans for anti-revolutionary Iranians based abroad” according to a local justice department official.\(^{43}\) At least one individual had participated in or led BBC-funded journalism workshops, which officials linked to British intelligence. Five individuals were kept in solitary confinement for four months and subject to daily interrogations. In June 2014, the revolutionary court in Kerman sentenced 11 individuals for “designing sites… for media hostile to the regime”: Honarmand to 11 years’ imprisonment, Vahedi (2.5), Hossein Nozari (7), Paknejad (5), and seven others to 1.5 years plus 3 years’ probation.\(^{44}\)

In July 2013 seven contributors to the Sufi website Majzooban Nor were convicted of producing antigovernment propaganda, insulting the Supreme Leader, and endangering national security. Hamidreza Moradi was sentenced to 10 years in prison, Reza Entesari was sentenced to 7.5, and Mostafa Daneshjo, Farshid Yadollahi, Amir Islami, Omid Behrouzi and Afshin Karampour were each sentenced to 7.5. The court banned them all from practicing any kind of political or journalistic activity for five years after their release. The defendants, who have been held in Tehran’s Evin prison since September 2011, and their lawyers refused to attend the trial on the grounds that it was unfair.\(^{45}\)

Even if access to social media is restricted in the country, numerous individuals have been targeted for their activities on Facebook and YouTube. In early September 2013, the IRGC arrested five administrators of popular Facebook pages. While the pages were not politically focused, Roya Irani,

\(^{41}\) Press Law, \url{http://press.farhang.gov.ir/fa/rules/laws2}.

\(^{42}\) Islamic Republic of Iran: Computer Crimes Law Article 19, January 30, 2012,


Amir Golestani, Fariborz Kardar, Massoud Ghasemkhani and Seid Massoud Seiad Talebi allegedly shared or posted information related to the opposition Green movement. According to Reporters Without Borders, they were charged by the Tehran prosecutor’s office with “meeting to conspire against national security” and, as of December 2013, were still held at Evin prison.

In a separate development from May 2014, eight individuals found guilty of blasphemy, spreading anti-regime propaganda, or insulting Supreme Leader Khamenei on Facebook and were sentenced between 7 and 20 years of jail time. Among those sentenced to 20 years was Roya Saberinejad Nobakht, a 47-year-old woman and British national. Gholam Hossein Mohseni Eje’i, the general prosecutor of Iran, separately announced the arrest and imprisonment of an individual responsible for setting up fake Facebook pages that claimed to represent members of Rouhani’s cabinet.

Even the most seemingly benign activities can provoke the ire of conservative authorities. Five dancers and one director were arrested for a homemade video posted to YouTube that featured men and women—the latter without headscarves—dancing together in a violation of conservative customs. The “Happy in Tehran” clip was one of hundreds of music videos set to the Pharrell Williams song “Happy” that have been reproduced around the world. The group was forced to repent on a national television, during which a police chief referred to the video as “a vulgar clip which hurt public chastity.” They six were later given suspended sentences of one year in prison and 91 lashes in September 2014.

Iranians in the expatriate community are also intimidated for their online activities. Prior to the elections, Radio Free Europe issued a statement criticizing the Iranian regime’s pressure on family members of Radio Farda staff. According to Radio Farda’s director, Arman Mostofi, relatives of staff members were summoned for interrogations and were told to advise their relatives to refrain from working with the organization.

Saeed Malekpour, a web developer who had previously been sentenced to death for blasphemy, had his sentenced changed to life imprisonment. Malekpour’s lawyer, Mahmoud Alizadeh Tabatabaee, told ISNA News Agency in August 2013, that after his death sentence was upheld at the Supreme Court, he repented and showed remorse, leading to his sentence reduction. He was arrested in 2008 after image software he developed was used in an adult website.

48 http://itna.ir/vdcbz9b5.rhbzpizuir.html
In March 2012, the Communications Regulatory Authority issued Bill 106, which required the registration of all IP addresses in use inside Iran. Implementing such registration will allow the authorities to track users’ online activities even more thoroughly and is a fundamental part of implementing the National Information Network. In addition, the sale and use of VPNs is illegal. Tehran’s Cyber Police (FATA) arrested a 35-year-old man for selling VPN access in 2014, noted that the suspect was found through “monitoring the web space.”

As of March 2012, customers of cybercafes must provide information including their name, father’s name, national ID number, and telephone number before using a computer. Cafe owners are required to keep such information, as well as customers’ browsing history, for six months. They are also required to install closed-circuit surveillance cameras and retain the video recordings for six months. Mehdi Mir-Mohammadi, head of the IT-Union of Tehran, commented that some elements of the regulations infringe on user privacy and could lead to new forms of cybercrimes.

In addition, the CCL obliges ISPs to record all the data exchanged by their users for a period of six months, but it is not clear whether the security services have the technical ability to process all this data. When purchasing a mobile phone subscription or prepaid SIM card, users must present identification, facilitating the authorities’ ability to track down the authors and recipients of specific messages.

Despite international legal restrictions placed on the selling of surveillance equipment to the Iranian government, there have been past reports that Chinese and some Western companies have been providing the Iranian authorities with technology to monitor citizens’ digital activities. Specifically, investigative reports by Reuters and the Wall Street Journal found that Huawei Technologies and ZTE Corporation, both Chinese firms, were key providers of surveillance technology to Iran’s government, allegations both companies have denied. According to an uncovered PowerPoint presentation outlining the system’s capabilities, Iran’s MobinNet ISP would potentially have the capacity to utilize deep packet inspection (DPI), real time monitoring of communication traffic, the ability to block websites, track users and reconstruct email messages as a means of monitoring citizens.

Filtering and arrests are supplemented by hacking and distributed denial-of-service (DDoS) attacks on the websites of government critics. In the lead up to the elections, websites critical of the government, including Khodnevis, Iran’s Communist Party, and Green Wave Voice were hacked.

---

56 “Internet cafes are required to authenticate users, all the pages viewed in the Internet cafes should be recorded”, Asriran, accessed June 24, 2013, see http://bit.ly/1lAheES.
Google also released a statement that it detected and stopped thousands of phishing attacks targeting email accounts of Iranian users ahead of the election. 60

Iran has significantly increased its hacking capabilities in recent years. According to a report published by FireEye, a digital security firm, in May 2014 the development of Iranian hacking capabilities, particularly its ‘Ajax Security Team’, is “consistent with Iran’s efforts at controlling political dissent and expanding offensive cyber capabilities”. However, the report noted that Iranian hackers are not necessarily directly linked to the government or the military. 61

There have also been several official plans to recruit and train cyber defense experts and hackers in the past. The Deputy of IT and Communications at Iran’s Civil Defense Organization announced that a Cyber Defense program of study would be introduced to some universities in the country on the graduate level. 62

According to Zone-H, a website dedicated to tracking hacking incidents, there were a total of 1,387 website defacements attributed to Iranian hackers during March 2013 alone, with a similar number in February. The majority of these are attributed to the Ashiyane Digital Security Team, which ranks as the second most active group in world, with defacements of thousands of websites linked to foreign governments and high-level organizations. 63  It is also noteworthy that the head of Ashiyane, Behrouz Kamalian, was sanctioned under the European Union’s human rights sanctions regime for being linked with the IRGC and responsible for a cyber-crackdown against domestic opponents and reformists, and foreign institutions. 64

Italy

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td>Free</td>
<td></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>6</td>
<td>6</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>23</td>
<td>22</td>
</tr>
</tbody>
</table>

Population: 59.8 million

Internet Penetration 2013: 58 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: No

Bloggers/ICT Users Arrested: No

Press Freedom 2014 Status: Free

* 0=most free, 100=least free

Key Developments: May 2013 – May 2014

- In a controversial plan, Italy’s communications regulator AGCOM empowered itself to make decisions to order the takedown of content and blocking of websites that violate copyright laws in a process that involves no judicial oversight. The move did not follow any parliamentary approval (see Limits on Content).

- Orders to block copyright-infringing websites increased dramatically over the past year, with one monitoring organization recording almost 450 blocked websites in Italy as of May 2014, up from less than 150 one year previously (see Violations of User Rights).

- In a positive ruling, Italy’s Supreme Court upheld a 2013 decision that stated three Google employees did not violate privacy protections and could not be held responsible for failing to obtain the consent of individuals featured in online videos posted to their site. The case revolved around a video, posted in 2006, that showed Italian schoolchildren bullying an autistic student (see Violations of User Rights).
Introduction

Italy’s internet penetration rate—which remained at around 58 percent this year—lags behind many other European countries.¹ Italian authorities do not generally engage in political censorship of online speech, and, as in previous years, no bloggers were imprisoned as of mid-2014. Despite a number of judicial decisions asserting that intermediaries are not liable for the content posted by users, overly broad interpretations of liability in defamation or intellectual property rights cases resulted in unusual judicial decisions and disproportionate burdens placed on online news providers. In the past, proposals have been put forward by past governments that raised alarm bells for free expression advocates.² This year, the central development has been the extension of the powers of the telecom regulator, the Authority for Communications (AGCOM), to order hosting providers to take down content if an internal administrative panel deems that it violates copyright protections. If no action is taken within 72 hours, AGCOM may order ISPs to block a website, even if hosted domestically, with no court order. Italy is reportedly the first European country to have such a regulation in force.³

After the general election of February 2013, a new government was formed under the young premier Enrico Letta, who promised to kick-start reforming the country. The government was backed by all the major parties, including Silvio Berlusconi who still owns, directly and indirectly, a private media conglomerate. Nonetheless, the government lasted less than a year. In December 2013, the center-left party held primaries that were won by Matteo Renzi, the mayor of Florence. Soon Renzi claimed the premiership and Italy’s youngest ever government, as measured by members’ average age, was sworn in. Berlusconi forged a tacit alliance with the new premier, after the media mogul was sentenced on charges of fraud and had to keep a low profile in politics.

If Berlusconi and his party, Forza Italia, no longer have the political power to steer through controversial initiatives such as the wiretapping bill, they still intend to check any move that might undermine Berlusconi’s position in the media market. Italy’s traditional media ownership has remained basically unaltered. Berlusconi’s center-right party still favors television interviews. Twitter, Facebook, and blogs are more effectively used by Renzi, as well as the populist leader Beppe Grillo.⁴

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. Remaining obstacles to greater internet penetration include users’ lack of familiarity

---

² 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.
⁴ Grillo’s blog is one of the most read, reported by and discussed in the traditional media in Italy. [http://www.beppegrillo.it](http://www.beppegrillo.it).
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.

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 2013-14, this attitude still wins through, but, as in the past, there is a considerable gap between aspirations and reality. According to the International Telecommunication Union (ITU), Italy had an internet penetration rate of 58.46 percent as of December 2013, an increase in 13 percent from 2008.\(^5\) While Italy’s internet penetration rate is higher than the global average, it is lower than the overall rate in Western Europe. A recent report shows it also lags behind Europe on many other ICT indicators.\(^6\) The relatively low penetration rate is not due to infrastructural limitations as much as unfamiliarity with the internet among the older generations and a general affinity for mobile phone devices rather than desktop computers.

According to data from January to March 2014, daily mobile users number more than household users by 14.5 million to 12.5 million.\(^7\) For fixed lines, Italians still prefer to access the internet 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.\(^8\) Cost is not a significant barrier to access. The price for a broadband connection may range from EUR20 to EUR40 (US$26 to S$52) per month. The average monthly per capita income is around US$2,700.\(^9\)

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 owns the physical network, but is required by European Union (EU) legislation to provide fair access to competitors. Telecom Italia began the process of spinning-off its business entity that deals with infrastructure at the end of May 2013.\(^10\) ADSL fixed broadband connections with basic service up to 2 Mbps are available on about 98 percent of Italy’s territory. However, fast broadband offering more than 30 Mbps is expected to reach 50 percent of the territory only in 2016 or 2017, and is now among the lowest in the EU.\(^11\) In October 2013, only 3.7 percent of Italians enjoyed speeds of over 10Mbps,


\(^8\) http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.


\(^11\) The EU Digital Agenda calls for 100 percent of the territory covered with 30Mbps and at least 50 percent with ultrafast (over 100Mbps) by 2020; Palazzo Chigi, “Rapporto Caio” Achieving the Objectives of the Digital Agenda for Europe (DAE) in Italy: Prospects and Challenges, 30 January 2014, http://www.governo.it/Notizie/Palazzo%20Chigi/dettaglio.asp?id=74619.
though this represents a 40 percent increase from 2012.\textsuperscript{12} There is no plan by telecom companies to achieve ultrafast broadband over 100 Mbps any time soon.

Mobile phone remains at almost 160 percent as of 2013.\textsuperscript{13} The majority of subscriptions are still prepaid, but flat tariffs are becoming more common.\textsuperscript{14} Telecom Italia Mobile (TIM), Vodafone, Wind, and 3 Italia are the major carriers, and all of them operate third-generation (3G) networks with 4G quickly replacing it. As in other countries, sales of tablet computers are on the rise among the younger generation and are likely to keep growing in the coming years.

An ambitious infrastructural plan entitled “Growth 2.0” was announced in 2012 with the aim of closing Italy’s “digital divide”, or regional discrepancies in fast internet access, within two years. In February 2014, the deadline was moved to 2015.\textsuperscript{15} The same plan included a “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 others).\textsuperscript{16} In June 2013, Enrico Letta, prime minister at the time, appointed Francesco Caio as the country’s commissioner for the digital agenda. Caio, a manager with extensive experience in telecoms, presented a comprehensive report in January 2014. As a result, the infrastructure and economic development minister, along with the ministries of the economy, research and university, public health, and others, were tasked with profoundly “transforming” Italy’s public administration.\textsuperscript{17} However, after the collapse of the Letta government, Caio left to become CEO of the national postal service Poste Italiane and the project was put on hold. Prime Minister Renzi has again emphasized the centrality of the digital agenda, but with the intermittent paralyses that characterize Italy’s political system, the country is unlikely to fulfill this EU goal.

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 public broadcasting. AGCOM’s president is appointed by the majority party or coalition in parliament. Past commissioners have come under pressure when it came to television broadcasts, particularly during Berlusconi’s premiership, but today the agency’s main priority is digital copyright, for which it has proposed a tax on all electronics products.\textsuperscript{18} Angelo M. Cardani, AGCOM’s current


\textsuperscript{14} AGCOM “Osservatorio Trimestrale sulle Telecomunicazioni”, 30 September 2013, \url{http://www.agcom.it/default.aspx?id=12264&Search=abbonati_mobile}.


\textsuperscript{16} Italian text at \url{http://www.gazzettaufficiale.it/moduli/DL_181012_179.pdf} See also \url{http://www.agenda-digitale.it/agenda_digitale/}.

\textsuperscript{17} “Rapporto Caio” Achieving the Objectives of the Digital Agenda for Europe (DAE) in Italy: Prospects and Challenges, 30 January 2014, \url{http://www.governo.it/Notizie/Palazzo%20Chigi/dettaglio.asp?id=74619}.

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.

\textsuperscript{18} Yahoo Finance, “Telefonini e musica, torna la tassa per i diritti d’autore?” , 5 March 2014, \url{https://it.finance.yahoo.com/notizie/telefonini-musica-torna-tassa-diritti-autore-155034196.html}.
Another important player in the field of communications is the Italian Data Protection Authority (DPA). Set up in 1997, the DPA 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 of data protection laws, as well as “banning or blocking processing operations that are liable to cause serious harm to individuals.”20 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.21 The clear privacy issues are one of the rationales for the consultation.

Limits on Content

The Italian authorities do not generally restrict political content, although there has been a dramatic increase in the amount of websites blocked on grounds of selling forged goods, illegal streaming, the downloading of copyrighted content, and unlicensed gambling. According to “Osservatorio Censura,” (Censorship Observatory), the amount of websites blocked in Italy rose from 149 in May 2013 to 439 in May 2014.22 Because of Italy’s civil-law system, some judges may occasionally issue rulings that impose responsibilities on intermediaries to regulate user-generated content, although other judges have repeatedly affirmed that intermediaries should not be liable for content posted by users. Italians have access to the full range of domestic and international news sources and human rights websites. The social-networking site Facebook, the Twitter micro-blogging service, the video-sharing site YouTube, and international blog-hosting sites are all freely available. Indeed, the use of social media has become a mandatory element of Italian politics, particularly over the past two years.

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.23 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 blocking.24 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

---

19 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; http://www.agcom.it/Default.aspx?message=contenuto&DCId=184.
22 See http://censura.bofh.it/grafici.html.
23 The blacklist is available (in Italian) at http://www.aams.gov.it/site.php?id=2484.
circumvention tools. ISPs also offer subscribers “family internet” packages that automatically block access to adult pornography and sites with violent content, in exchange for a small premium.

In December 2013, AGCOM granted itself the power to order content hosts to take down sites or remove content if a review by an internal administrative panel detects a violation of copyright.\(^{25}\) If no action is taken within 72 hours, AGCOM may now order ISPs to block offending websites with no need for a court order. The new regulations also allow punishments of up to EUR 250,000 for users uploading copyright-infringing content and for ISPs failing to comply with the orders in a timely fashion.\(^{26}\) The controversial plan, which has been strongly criticized by users’ organizations and ISP representatives for lacking a requirement for prior judicial approval, entered into force on March 31, 2014.\(^{27}\) It did not come under parliamentary review.\(^{28}\) AGCOM’s mandate includes sites that contain links to other websites that provide copyrighted-infringing content, as well as the hosts. However, when the first orders went out at the end of April, it became apparent that all of the targeted websites were hosted outside of the country, thus limiting the reach of the Italian authorities. For this reason, AGCOM invited Italian ISPs to block access to those sites on the basis that the court order would “eventually” arrive.\(^{29}\) This would give ISPs a highly discretionary power, without a judicial order or ruling, to filter access.\(^{30}\)

Consumer rights organizations and ISP associations are worried that the procedures may end up unjustifiably inhibiting users from accessing content that they have uploaded to the web but legally own. Of further concern is the fact that links to legal content can also be removed or rendered inaccessible if the authority overreaches in its duty. On April 9, 2014, the administrative court of Rome ruled that opposition to the resolution was justified and asked AGCOM to begin a moratorium on the process until June 2014 pending further consideration and examination. AGCOM, however, decided to proceed with their plans and to run the risk that, after a future contrary ruling, its executive decisions may all be found void and unlawful.\(^{31}\) Laws passed in 2000 and 2003 gave AGCOM an executive mandate to act in violations of copyrights.\(^{32}\)

These developments come after the European Court of Justice ruled that national courts may order ISPs to cut off users’ access to copyright-infringing websites. In the case, involving a German-Austrian film company and an Austrian ISP, the ECJ clarified that ISPs can be considered

---


intermediaries and should prevent access to an offending website in a way that balances the right to information with intellectual property rights.\textsuperscript{33}

At times, Italian authorities continue to request the removal of specific content, although the amount is limited. According to Google, the government issued 27 court orders for 135 items to be removed between January and June 2013 (compared to 23 requests over the previous six months), as well as 6 requests from executive bodies such as the police or regulating agencies.\textsuperscript{34} Nearly half of the requests were accepted and involved material that was broadly interpreted as defamatory.

Decisions related to the blocking of websites for copyright violations are implemented by the Guardia di Finanza (GdF, Finance Guard), which handles issues of cybercrime, fraud, and trafficking.\textsuperscript{35} 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 communications.\textsuperscript{36} Nonetheless, many in the Italian legal community now believe that, based on existing jurisprudence and thanks also to the provisions laid out in the EU e-Commerce Directive,\textsuperscript{37} service providers are not required to censor search results. Likewise, since 2011, when Italy’s Supreme Court declared that editors of online magazines were not responsible for defamatory comments posted by readers (thus taking note of 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. In 2011 and 2012, however, cases of defamation have been brought against online content providers and intermediaries that have led to the blocking or filtering of ICT content.\textsuperscript{38} This legal uncertainty is due, in some part, to the inability to create new laws to compete with the fast changing technology. Existing laws are applied in a contradictory manner and are often overturned at every appeal, resulting in extended legal battles.

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.\textsuperscript{39} Thus RTI-Mediaset won the case and ten indexing platforms with links to major sports streaming websites were shut down. This decision was reiterated again in September 2013 again by

\begin{itemize}
\item \textsuperscript{34} Google “Rapporto sulla trasparenza, http://www.google.com/transparencyreport/removals/government/countries/?p=2013-06.
\item \textsuperscript{35} 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://punto-informatico.it/3768010/PI/News/italia-maxisequestro-dello-sharing-corso.aspx.
\end{itemize}
a court in Rome that ruled that providing links to the streaming of soccer games 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*.40

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.41 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.

Following the European Union principle on “the right to oblivion” (or “the right to be forgotten”), in April 2012, the Supreme Court imposed an obligation on publishers to update their online archives to ensure that outdated facts do not inadvertently damage someone’s reputation. Furthermore, on May 13, 2014, the European Court of Justice found that the 1995 Data Protection Directive did apply to the activities of search engines like Google, and that these companies may have to remove certain search results if the data is deemed to violate an individual’s right to privacy.42 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.43

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 now 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. As of end of 2013, the country was home to over 26 million Facebook users (42.4 percent of the population, up more than 5 percent from 2012), the 11th highest number in the world.44

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.45 The Five Star Movement, 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 movement used the internet both to strengthen their political basis and to survey it. The Five Star Movement used the web and social media (1) to select its candidate for the Italian presidential election,46 (2) to vote on expelling party members, such as those MPs who do not conform to the movement’s rules and internal decisions, and (3) to provide an outlet for Grillo’s announcements and statements.47

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, data transparency is mostly a declared “intention” than a real, sanctioned obligation.48 As of mid-2014, the government has opened a dedicated web site that offers data and information voluntarily made available by local and central administrations.49 Such tools, while valuable for scholarly research, is still a far cry from constituting an Italian FOIA.

Violations of User Rights

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.50 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 (see “Limits on Content”). For this reason, online free expression advocates have focused their efforts on proposing

44 . “Italy”, Social Times Daily. 10 September, 2013, http://it.socialtimes.me/stat/IT.
46 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.
47 See Grillo’s blog at http://www.beppegrillo.it/. Grillo was criticized even on his blog for the advertisements revenues from his blog.
legal amendments to improve protections and prevent censorship rather than engaging in public interest litigation.  

In a positive ruling this February, Italy’s Supreme Court found that three Google employees were not liable for failing to prevent the uploading of a video of Italian schoolchildren bullying an autistic student. The employees were initially handed six-month suspended sentences for a criminal breach of privacy laws in 2010. Italy’s highest court agreed with the 2013 decision of an appeals court, which ruled that Google could not be held responsible for obtaining the consent of any individuals that may feature in videos uploaded to the site.

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 a chilling effect on journalists and their editors. As of May 2014, there have been extremely few libel suits against bloggers and other online writers in Italy.

Concerns exist over the disproportionate use of Italy’s libel law over Facebook. In early 2013, a young woman who posted negative and racist remarks about her former employer on the social network and was found guilty of libel and made to pay a EUR 1,000 fine. The prosecution successfully argued that libel can occur so long as the offense occurs through any medium, online or traditional, that can reach a larger public. Further, a third-level appeals court found a non-commissioned GdF officer guilty of libel for posting negative comments about a colleague on Facebook, even though the latter’s name was never mentioned in the post. 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.

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.

51 Andrea Monti (lawyer specialized on Internet freedom and activist), in a conversation with author, February 20, 2012.
overall perception is that the country’s authorities are engaged in a large number of wiretaps, although this may only be a perception. On the other hand, it is undeniable that news media regularly publicize wiretap information that is leaked to them and attempts to prevent the publication of wiretaps through the imposition of fines have failed.

In March 2008, the parliament approved a law (No. 48 of 2008) to ratify the Council of Europe’s Convention on Cybercrime, which established how long internet-related communication data should be retained. This matter was further refined with the inclusion in the Italian legislative system of the 2006 EU Data Retention Directive. Under the current legal framework, ISPs must keep users’ traffic records—though not the content of communications—for 12 months. This includes 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.

Data retention practices in Italy 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 Charter of Human Rights. The ruling was lauded among privacy proponents who had long argued that requirements for the blanket retention constituted mass surveillance and far exceeded what was necessary for law enforcement purposes. However, the decision has also prompted debate among legal experts, 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. The situation remains unclear in Italy, although Italian ISPs routinely retain data for a variable amount of time.

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, 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 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

57 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.


60 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.

advertisement companies. 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. 

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. In 2013, according to intelligence reports, there were increasing fears that the country's economic crisis might push extremist groups to adopt cybercrime or cyberterrorism as a form of protest. Despite the increasing emphasis on cybersecurity, in May 2013, the Italian Ministry of Interior was nevertheless attacked by the Italian branch of Anonymous as retaliation for the arrest of some cyberactivists only a few days earlier. The country’s official cybersecurity strategy was published in December 2013.

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. More common is the defacement or launching of denial-of-service (DoS) attacks against websites—mostly government-linked ones—as a form of political protest. 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.


63 “Ulteriore Deroga fino a fine giugno 2012 per la casella PEC aziendale,” IlSoftware.it, http://www.i-node.it/2012/05/ulteriore-deroga-fino-fine-giugno-2012-la-casella-pec-aziendale/.

64 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://daily.wired.it/news/internet/hacking-accordo-tra-symantec-e-polizia-postale.html; Alessandra Talarico, “Cybercrime. Italia vittima e carnefice: è il paese che più abbocca al phishing e tra i più attivi negli attacchi web based” [Cybercrime. Italy Victim and Victorizer: 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://www.key4biz.it/News/2010/04/22/e-Security/cybercrime_botnet_spam_ebanking_social_network_spyware_adware_phishing.html.


68 The Police and the judiciary are often targeted, see for example Corriere della Sera “Gli hacker colpiscono ancora: attaccato sito della polizia campana” February 17, 2013, http://www.corriere.it/cronache/13_febbraio_17/polizia-hacker-anonymous_1727d948-790b-11e2-a299-b72f93ae99be.shtml.

69 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, http://globalsecuritymap.com/it, accessed 19 May 2014.
Japan

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>7</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>22</td>
<td>22</td>
</tr>
</tbody>
</table>

Population: 127.3 million

Internet Penetration 2013: 86 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: No

Bloggers/ICT Users Arrested: No

Press Freedom 2014 Status: Free

* 0=most free, 100=least free

Key Developments: May 2013 – May 2014

- Politicians embraced social media to campaign during July 2013 senate elections after outdated restrictions on digital electioneering were revised in April (see Limits on Content).

- A state secrets law introduced 10-year jail terms for leaking or publishing classified information in December 2013, despite local and international concerns about its overbroad definitions and lack of oversight (see Violations of User Rights).

- The May 2013 “My Number” law will track residents’ access to government services via electronic ID cards from 2015, prompting fears about data security (see Violations of User Rights).
Japan

Introduction

The use of the internet as a political communications tool expanded during the coverage period of this report. July 2013 saw the first elections since Prime Minister Shinzo Abe revised restrictions on online campaigning in April. Abe's Liberal Democratic Party (LDP) won control of the senate, consolidating a resounding victory in the 2012 general election.

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 80 percent. Major Japanese companies such as Nippon Telegraph and Telephone Corporation (NTT) and Fujitsu offered ISP services in the 1990s, while mobile carrier NTT DoCoMo pioneered the world's first large-scale packet-based mobile internet service, i-mode, in 1999. Despite strong access and a broad lack of content restrictions, 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 December 2013, prompting street protests in the capital supported by social media users around the country. The legislation, which criminalized both leaking and publishing ill-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 July 2014 in a review of Japan's human rights practices, 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.”

Data security also made headlines. A new law introduced ID numbers for Japanese residents, to be stored electronically and linked to personal social security and healthcare information, sparking privacy concerns. Police and ministers consolidated initiatives to combat domestic and international cybercrime, and in June 2013 the Chief Cabinet Secretary announced the creation of the post of Cabinet Information Communications Policy Officer. Yet many feared the new ID system would be vulnerable to cyberattacks or improper access by corporations, after news reports documented private sector players sharing consumers’ digital records without informed consent.

Obstacles to Access

In general, Japanese people experience few obstacles to internet access. Internet penetration among households overall in 2013 remained slightly over 86 percent, and 97.8 percent for businesses.

---

Japan

During 2013, mobile access continued to increase among Japanese internet users utilizing various appliances. Smartphones were particularly popular, surging in growth from 49.5 percent in the previous year to 62.6 percent. Tablet utilization also grew from 15.3 to 21.9 percent. The popularity of internet-enabled game consoles connected to television sets, also known as “family computers” in Japan, also increased from 29.5 percent in 2012 to 38.3 percent as of the end of 2013. Dial-up internet connections plummeted from 11.6 percent in 2012 to 1.9 percent by the end of 2013, while broadband connections grew by almost the same amount from 79.2 percent to 88.5 percent during the same period. Access is high quality with competitive speeds. While landline or fixed phones showed a very slight decrease—from 79.3 percent to 79.1 percent—fax machines usage grew from 41.5 percent to 46.4 percent during 2013.

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.

Mobile penetration reached 109 percent in 2013. Increasing smartphone use has made the market more competitive. Japan has four major mobile operators, but the top three—KDDI Au, NTT Docomo, and Softbank—all use the CDMA wireless network or a variant. Domestic coverage is extremely high. The fourth carrier, Y!Mobile, was formed in August 2014 from a merger of two companies: Emobile, formerly a 3G company that had an agreement with Docomo for roaming, and Willcomm, which was a PHS carrier offering an affordable alternative to CDMA with more limited range. In early summer 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. According to 2013 data published, the average household in Japan spends around JPY 6,925 ($69) for mobile service per month, or JPY 83,099 yen ($830) per year.

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.
Asymmetric regulation, which creates stricter rules for carriers with higher market share, helped diversify the industry, though critics say the expense of switching providers—and the inconvenience of losing an email address and other services—ties customers to the dominant players and creates a barrier for new entrants. While the telecommunications market looks open, therefore, with hundreds of providers offering FTTH, DSL, CATV, FWA, and BWA services, the NTT group remains dominant in practice. No major foreign operators have successfully penetrated the telecommunications market, with the exception of smartphone devices manufactured by Apple and Samsung, though many invest in, or partner with local providers. Competition between Softbank, formerly the exclusive provider of Apple’s iPhones, and the NTT group intensified with NTT Docomo’s announcement in September 2013 that it reached an agreement with Apple to add iPhone handsets and iPads to its mobile product lineup.

There are few infrastructural limitations on internet access in Japan. However, a dual system of mobile communications has existed since the introduction of NTT Docomo’s i-mode service. The capability to access the internet through mobile phones has existed since 1999, and flat-rate data plans have been available since 2004. For that reason, there has been little demand for enhancing Wi-Fi access.

In the past two years, with the rapid increase in the number of smartphone and tablet users, calls for increased Wi-Fi access have been growing. In June 2013, NTT’s Docomo announced an expansion in LTE base stations to augment its Xi LTE and FOMA 3G services. Providers such as Asahi-net offer WiMAX plans with mobile routers capable of accessing multiple networks throughout the country. The private Wire & Wireless offers free Wi-Fi access in restaurants, coffee shops, and some train stations; registration requires an email address.

The vulnerability of Japan’s communication network became apparent in March 2011, when an earthquake and tsunami hit Japan’s east coast and caused a nuclear disaster. 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.

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 December 2012, and January and April 2013. NTT Docomo also dealt with four interruptions in July and August in 2012 alone. Fewer disturbances were reported during the coverage period.

Japan

There is no independent regulatory commission in Japan, though observers believe that the industry has generally improved in the past 12 years under the Ministry of Internal Affairs and Communications (MIC), which regulates the telecommunications, internet, and broadcast sectors.²⁶ 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.²⁷

Limits on Content

Politicians embraced social media to campaign during the July 2013 Upper House elections after outdated restrictions on digital electioneering were revised during the previous coverage period. Activists and civil society also used digital tools to promote local civic causes. Hate speech promulgated by nationalistic right-wing (netouyo) commentators against South Korean residents of Japan spread online, but so did counter-campaigns to combat racism. During a November 2013 protest against state secrets legislation in the capital, Twitter users expressed support nationwide.

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.²⁸ 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.²⁹ Otherwise, individuals or police instruct ISPs to administratively delete contested or illegal content. 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.³⁰ While the center received a record high of 196,474 calls in 2012, according to its annual statistics report for 2013, it received 130,720 reports from January to December 2013.³¹ Their breakdown of reports by type includes 22.7 percent involving illegal information (information involving illegal activities such as public displays of obscene materials or “publicly inciting or soliciting others to abuse controlled substances”), 2.6 percent involving harmful information (information that could invite illegal conduct, related to suicide, or which is “difficult to judge as illegal but seems to be illegal”), and 74.7 percent which “were beyond scope of its operational guidelines, including defamation, slander, murder notices, intellectual property infringement, information inappropriate for children, and other cases.”³² Providers are not obliged to

²⁶ Before 2001, regulation was managed by the now-defunct Ministry of Post and Telecommunications, and before that, the Diet.
Japan

comply, but most cooperate.

The 2001 Provider Liability Limitation Act directed ISPs to establish a self-regulatory framework to govern take-down 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 within two weeks. 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 practice, many citizens say service providers have failed to remove libelous content.

Police sometimes intervene more directly, and their emphasis on security over transparency occasionally threatens internet freedom. In April 2013, they recommended ISPs and website administrators cooperate to block IP addresses used by Tor—which allows internet users to disguise their location by connecting through a network of other computers—in order to prevent criminals from abusing the service, which also has many legitimate applications.

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. In 2012, game developers Gree and DeNA Mobage voluntarily adopted caps on purchases of virtual items by minors instead. 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.\footnote{Enigmmax, “Jail For File-Sharing Not Enough, Labels Want ISP-Level Spying Regime,” TorrentFreak, June 24, 2012, https://torrentfreak.com/jail-for-file-sharing-not-enough-labels-want-isp-level-spying-regime-120624/}

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 II. 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.

YouTube, Twitter, and international blog-hosting services are freely available, as are popular domestic platforms like Nico Nico Douga, a video-sharing site, and LINE, a chat application launched in 2011.

In late 2013 and early 2014, the use of the internet as a public relations and communications tool by high-level politicians and national-level ministries continued to increase. One engineer ranked their popularity during July 2013 elections for the upper house, the first to take place with no limits on digital campaigning immediately before the polls.\footnote{See, http://globalvoicesonline.org/2013/07/15/web-popularity-of-japans-candidates-ranked/} In addition to the prime minister’s official Facebook page, the Ministry of Foreign Affairs Japan (MOFA) created general accounts, as well as for specific programs and embassies, on Twitter, Facebook, YouTube, and Flickr.

Japan’s stance on foreign relations was also communicated to an international internet audience. In a nod to the importance of foreign relations with China, MOFA also opened accounts on Chinese social networks such as Sina Weibo and Douban.\footnote{See, http://www.mofa.go.jp/about/list_en.html} In the aftermath of the controversy following the posting of a video on YouTube showing a collision between Japanese Coast Guard vessels and a Chinese fishing boat,\footnote{See, http://sinosphere.blogs.nytimes.com/2014/02/13/japan-presses-claim-over-2010-collision-with-chinese-fishing-boat/?_php=true&_type=blogs&__r=0} MOFA posted two 90-second video clips to a YouTube channel that represented Japan’s historic relationship with the disputed Senkaku Islands (Diaoyu Islands).\footnote{See, http://www.scmp.com/news/asia/article/1339090/japanese-youtube-videos-diaoyus-claims-anger-china?page=all}

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,” CPJ Blog, April 14, 2011, http://www.cpj.org/blog/2011/04/nuclear-reporting-freelance-censorship-allowing-threat.php; 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,” press release, April 6, 2011, http://www.soumu.go.jp/menu_news/s-news/01kiban08_01000023.html} though the national
police agency reported 41 items for review.\(^{46}\) Others found an outlet to report on the aftermath of the disaster online.\(^{47}\)

Some news reports from the past year expressed concern about nationalistic discourse by Japanese web trolls, or netouyo, escalating into hate speech online, particularly targeting South Koreans and Chinese communities amid territorial disputes between Japan and their respective governments.\(^{48}\) Abe’s stance on these active rivalries, as well as historic ones, does nothing to calm the situation. In December 2012, he said he was reconsidering apologies Japan had made for acts of wartime aggression, including one for forcing Asian and European women to work in army brothels, which he denied was coerced. While he later retracted this position,\(^{49}\) an advertisement with a government seal that appeared to support such a revisionist history was widely circulated on social media in 2013, though it turned out to be a fake.\(^{50}\) The incitements to violence directed at South Korean and Chinese people—and unpatriotic activity in general—which flourished on websites like 2channel, were far more extreme, but they were arguably rooted in the same nationalist discourse, which threatens to undermine the diversity of voices being heard in Japanese cyberspace.\(^{51}\)

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,\(^{52}\) 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.\(^{53}\) 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 discriminate against new media practitioners. In 2012, at least one online journalist was denied access to one of their Tokyo locations,\(^{54}\) 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.\(^{55}\) In the meantime, independent online news outlets have struggled to sustain themselves financially. OhmyNews, a South Korean platform, established a Japanese operation in 2006, but closed in 2008. The U.S.-based Huffington Post digital media website launched a Japanese-language version in May 2013.\(^{56}\)
Much digital activism was also effective at a local rather than a national level, including maps sharing public information about disaster relief.\(^5\) During the coverage period, activists also monitored online slurs and used digital tools to map racist graffiti proliferating in Tokyo.\(^6\) One movement with a wider reach was a November 2013 protest against state secrets legislation. While street protests were concentrated in the capital, Twitter users around the country expressed support with hundreds of thousands of messages.\(^7\) In September 2014, outside the coverage period of this report, the government tabled draft revisions to the legislation after soliciting comments from the public in August.\(^8\)

**Violations of User Rights**

In December 2013, Japan passed an unpopular state secrets law carrying prison sentences of up to 10 years for individuals who publicize classified information—regardless of whether or not they expose wrongdoing. Objectors said it was hurried through by the administration, which gained overbroad powers to categorize information as secret and to adjudicate over alleged leaks without independent oversight. News reports said police detained at least 20 people under a punitive copyright law during the coverage period, but no disproportionate sentences were reported. Despite growing concern about cybersecurity in Japan, the Diet, Japan’s bicameral parliament, passed a “My Number” law in May 2013 which will introduce ID numbers tied to electronic data chips as a means to access government services for residents of Japan in 2015. Privacy advocates said legislation to protect individuals was falling behind such digital solutions, illustrated in Tokyo in 2014 when supermarkets were reported sharing security camera images of customers through an electronic network without consent.

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.”\(^9\) In general, individuals and media can exercise this in practice, though social and legal constraints exist.

In July 2013, the LDP won the senate after gaining a landslide electoral victory in the lower house of parliament, in December 2012.\(^10\) In May 2012, while still in the opposition, the party had proposed revising the constitution.\(^11\) Critics said their draft promoted conservative nationalism, replacing the subject of the constitution—currently the people of Japan—with the nation state, and subjugated

---


“freedoms and rights” to “public interest and public order.” While the revision, which would have required a significant political mandate, was abandoned, the LDP-majority parliament adopted a regulation to reinterpret a post-war constitutional limit on Japanese intervention in overseas conflict in mid-2014, part of a strategy to strengthen national security.

One facet of that strategy had implications for digital freedom of expression. The Act on the Protection of Specially Designated Secrets passed in December 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 and any one of the categories of defense, foreign affairs, “prevention of designated harmful activities” (such as “counter-intelligence”), and prevention of terrorism. 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. For those people who handle such state-designated secrets, intentional leaks are punishable by up to 10 years in prison and unintentional by up to 2 years, while 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. Draft revisions announced in September 2014 could address some elements that were subject to critique, if passed.

A 2013 revision of the Public Offices Election Act undid long-standing restrictions on use of the internet for election campaigns for the first time. 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. While these provisions were contested and revisions are still planned, news reports during the coverage period said politicians violating these restrictions face a potential JPY 300,000 ($3,060) fine or one year in prison; imprisonment would strip them of political rights to vote or run for office. Voters found improperly soliciting support for a candidate via email could be fined JPY 500,000 yen ($5,100) or jailed for two years, which would also deprive them of political rights. However, no citizens faced politically motivated arrest or prosecution for content they have published online during the coverage period.

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

68 See, http://www.kantei.go.jp/jp/topics/2013/headline/houritu_qaiyou_e.pdf#page=6&zoom=auto,-8,62
Japan

has been illegally copied, as opposed to those engaged in piracy for commercial gain. 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 ($102,000), the version in effect since October 1, 2012 added two years in jail or fines up to JPY two million ($20,500) for downloading a single file. The Japanese Bar Association said that downloading, as an essentially insignificant personal act, should be regulated by civil, instead of criminal laws. Some news reports said police conducted an antipiracy crackdown, arresting at least 19 people nationwide in February 2014. Details of the detainees’ activities were not publicized and no disproportionate sentences were reported.

Article 175 of the Japanese penal code bans the sale or distribution of broader categories of obscene material, and while it dates from over 100 years ago, it is considered to apply online. However, it does not define what constitutes obscenity, leading to concerns that it may infringe on artistic expression and LGBT rights. At the same time, Japan lacks restrictions on child pornography and hate speech online, which are acceptable to limit under international law. Laws passed in 1999 and 2003 outlawed the production, distribution, and sale of hardcore child pornography, including electronically, but possessing it for non-commercial use remains legal except in Kyoto prefecture, central Japan, where police arrested three people for purchasing child pornography online for the first time in September 2012 under an ordinance in effect since the previous January. Although nationalistic hate speech and incitement to racially motivated violence is proliferating online, the government has taken no action to curb it on grounds it is already criminalized under the penal code; yet police in 2012 were more likely to use the relevant clauses to prosecute antinuclear demonstrators than groups with on- and offline slogans that included exhortations to “kill Koreans.”

83 Tessa Morris-Suzuki, “Freedom of Hate Speech.”
Japan

Japan’s Supreme Court protects privacy through its interpretation of Article 13 of the constitution, which provides for the right to life and liberty.84 “Secrecy of communication” is also protected under telecommunications laws,85 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.86 A law enacted in 2003 and revised in 2008 prohibits electronic communications encouraging sexual activity with minors.87 Under the law, all online dating services must register with 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.88 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,89 lawmakers were seeking to expand it in December 2012.90 Critics say the law does not prevent the systematic storage of intercepted communications or protect innocent parties.91 Security agents and the military have been accused of implementing surveillance in cases involving national security.92

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. Law enforcement requests for this data should be supported by a warrant. In April 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. While the businesses cited security measures, 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. Japan Railways East (JR Higashi Nihon) also sparked a debate over privacy and consent when it announced that it would be offering anonymized data collected through prepaid IC fare cards (SUICA cards), to third-party companies.

A “My Number” law proposed by the cabinet in 2012 passed the Diet on May 24, 2013. Under this system each resident (including non-Japanese residents) will be assigned a unique ID number, from October 2015. 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. 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). 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.

Similar privacy debates focusing on the “My Number” system were ongoing during the coverage period. Politicians and bureaucrats said personal identification numbers would streamline social benefits and maintain accuracy and fairness in the provision of government services, as well as assist in identifying individuals in the case of natural disasters. The benefits that the new system would bring to Japan’s IT industry were also highlighted. However, the system’s opponents

99 See, http://www.japantimes.co.jp/opinion/2013/05/30/editorials/my-number-is-dangerous/#.Uzo5s1fh3Hg.
104 See, http://www.japantimes.co.jp/news/2013/05/10/national/lower-house-passes-my-number-bill/#.Uzo5ulfh3Hg.
105 See, http://www.japantimes.co.jp/opinion/2013/03/25/commentary/risks-of-using-my-number/#.Uzo5tlfh3Hg.
cited the potential for the leakage of personal information and identity theft, as it remains unclear how the data would be stored in order to provide services offered through multiple levels of government.\textsuperscript{106} The Japan Federation Bar Association in 2012 highlighted the system’s possible privacy issues when the bill was first introduced.\textsuperscript{107} In May 2013, the Japan Medical Association also contested the new system based on security issues involving medical records.\textsuperscript{108} 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.\textsuperscript{109}

No physical violence has been reported against bloggers or internet users in relation to their online activity.

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,\textsuperscript{110} they are not known to have been used to systematically target individuals or civil society groups.

In May 2013, the Kanagawa and Osaka police departments established separate divisions for addressing cybercrime,\textsuperscript{111} adding to police departments in Tokyo and 12 other prefectures.\textsuperscript{112} In June, the Abe administration added the legislative position of “Chief Information Officer” to the national-level cabinet;\textsuperscript{113} and the Information Security Policy Council within the National Information Security Center released a 55-page report entitled “Cybersecurity Strategy,” setting out basic principles including “ensuring a free flow of information” and “responding to increasingly serious risks” online.\textsuperscript{114} Japan also held bilateral talks with the U.S. concerning cybersecurity mid-year,\textsuperscript{115} culminating in a joint statement released by the U.S. Chamber of Commerce in Japan and the national business federation Keidanren pledging cooperation in cross-border data flows.\textsuperscript{116} This was followed by a second strategic plan entitled “International Strategy on Cybersecurity Cooperation – j-initiative for Cybersecurity,” which set out general principles for responses to cyber incidents and called for international rulemaking for cybersecurity.\textsuperscript{117}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{106} See, \url{http://www.japantimes.co.jp/opinion/2013/05/30/editorials/my-number-is-dangerous/#.Uzo5s1fh3Hq}.
\item \textsuperscript{108} See, \url{https://www.eff.org/deeplinks/2012/06/japan-national-id-proposal-spurs-privacy-concerns}.
\item \textsuperscript{109} See, \url{http://www.japantimes.co.jp/opinion/2013/05/30/editorials/my-number-is-dangerous/#.Uzo5s1fh3Hq}.
\item \textsuperscript{110} “Over 1,000 targeted cyber-attacks hit Japanese entities in 2012,” \textit{Japan Times}, March 1, 2013, \url{http://www.japantimes.co.jp/news/2013/03/01/national/over-1000-targeted-cyber-attacks-hit-japanese-entities-in-2012/#Uh-e28ukpTY}.
\item \textsuperscript{111} See, \url{http://japandailypress.com/japanese-police-beef-up-in-the-fight-against-cyber-crime-1130387/}.
\item \textsuperscript{112} See, \url{http://japandailypress.com/japans-national-police-authority-launches-cyber-defense-center-1729052/}.
\item \textsuperscript{113} See, \url{http://japan.kantei.go.jp/tyoukanpress/201306/04_a.html}.
\item \textsuperscript{115} See, \url{http://japandailypress.com/us-japan-hold-1st-comprehensive-cybersecurity-talks-0928570/}.
\item \textsuperscript{116} See, \url{http://www.keidanren.or.jp/en/policy/2013/090.html}.
\item \textsuperscript{117} See, \url{http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf}.
\end{itemize}
\end{footnotesize}
Jordan

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>13</td>
<td>15</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>46</td>
<td>48</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 7.3 million

Internet Penetration 2013: 44 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- On June 2, 2013 the Department of Press & Publications requested that the TRC order ISPs to block more than 200 websites for failing to comply with registration and licensing requirements set forth in the amended Press and Publications Law (see Limits on Content).

- A new anti-terrorism law was passed in April 2014. The law broadens the definition of terrorism in a way that threatens free speech and may be used to prosecute users and online journalists for anything broadly interpreted as damaging to Jordan’s relations with foreign governments (see Violations of User Rights).

- On September 17, 2013, the publisher of a Jordanian news outlet, Jafra, and its editor-in-chief were arrested under the penal code for publishing a third-party YouTube video which was deemed offensive to the Crown Prince of Qatar, Jassim Bin Hamad al-Thani. In the video the prince appears sitting, dancing and bathing with a group of women (see Violations of User Rights).

- Ayman al-Bahrawi was charged with “lengthening the tongue” and “insulting” foreign heads of state in private Whatsapp messages found on his mobile phone (see Violations of User Rights).
Introduction

Internet freedom conditions in Jordan have declined over the past year. Over 200 websites were blocked in June 2013 for failing to obtain a license from the Department of Press and Publications after the expiration of a nine-month grace period granted by authorities. In the ensuing months, many websites were unblocked after successfully obtaining a license. Nonetheless, new anti-terror measures passed in April of this year have worried opposition voices that authorities will use the legislation to silence dissent and further intimidate activists. Two journalists were brought before a state security court after posting a YouTube video of a Qatari prince, while an ordinary user was also arrested for private WhatsApp messages in which he criticized the Egyptian military’s takeover of power in that country. The increased restrictions came as Jordan continues to host at least 600,000 Syrian refugees amid prolonged insecurity over the threat of armed extremists in neighboring Syria and Iraq.

Low-level public protests have ensued since 2011 over both political reform and socio-economic conditions. 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 under an improved electoral framework in January 2013. That June, King Abdullah II released a “discussion paper” on liberalization and political reform in Jordan while also calling for “greater activism and citizen empowerment”. However, these developments have not significantly altered the status quo in the country. The Islamic Action Front, Jordan’s branch of the Muslim Brotherhood, once again boycotted the elections over political grievances and concerns over the elections law. 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.

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 sector. The TRC has subsequently played a crucial role in the development of the internet in Jordan, facilitating the provision of internet services to the population. However, the rise of political and social unrest in the region, coupled with the increasing influence of extremist organizations and the need for national security, has led to a tightening of internet regulations in Jordan. The authorities have been particularly sensitive to any perceived threat to national security or public order, leading to numerous instances of internet shutdowns and the blocking of websites deemed to be critical or subversive.

communication technology (ICT) sector. Recognizing the economic potential of the internet, authorities actively promoted ICT development in the small kingdom. Once seen as a means of 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. Likewise, 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.

Obstacles to Access

According to the International Telecommunication Union (ITU), a total of 44 percent of the Jordanian population accessed the internet by the end of 2013, up from 23 percent five years earlier. National figures from the Telecommunications Regulation Commission (TRC) estimated the number of users to have increased in the second quarter of 2014 to 73 percent, or 5.4 million users. Given the large number of people accessing the internet at cybercafes and offices, most users have access to broadband rather than dial-up connections. According to TRC statistics, the number of mobile broadband subscriptions reached over 1.2 million in the second quarter of 2014, with ADSL next at around 208,000. Most internet users are young people from ages 15 to 24.

Mobile phone use has also expanded rapidly and by the end of 2013, the number of subscriptions was over 10.3 million, representing a penetration rate of 141.80 percent. 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, Umniah. A call from the TRC to introduce a fourth mobile operator in December 2012, however, was rejected by Zain and Jordan Telecom. No new providers have been introduced since then and the three companies have a similar share of the market.

---

10 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).
14 Telecommunications Regulatory Commission of Jordan’s official website.
Jordan

After rejecting two international operators, the Jordanian government awarded Zain Jordan with the rights to introduce 4G services to the market. Zain has since announced that 4G service will be available by the end of 2014.\(^{21}\) A few weeks later, Mohamad Taani, TRC chief commissioner, was reported to have invited the other two major operators in Jordan, Orange Jordan and Umniah, to bid for 4G service frequencies.\(^{22}\)

The expansion of fixed-line internet access has been hampered by the relatively high costs of computers and connectivity. Indeed, fixed broadband subscriptions have decreased since 2009, with only 2.83 subscriptions per 100 inhabitants.\(^{23}\) On the other hand, mobile broadband use has soared to over 1.2 million subscribers.\(^{24}\)

For several years, internet connection fees were considered high relative to neighboring countries and the cost of living. Prices have decreased, reportedly upon direct orders from the king, but complaints about the quality of service persist. Monthly fixed-line subscription prices currently range from JOD 13 (US$18) for speeds of 128 Kbps and an allowance of 10 Gigabytes (GB), to JOD 65 (US$92) for speeds of up to 24 Mbps and a 65 GB allowance. Postpaid monthly plans for Evolved High-Speed Packet Access (HSPA+) range from JOD 5 (US$7) to JOD 49 (US$69) per month, depending on speeds and data allowances.\(^{25}\) By comparison, gross national income per capita is US$4,950, or US$413 per month.\(^{26}\) Meanwhile, internet access in many governorates and remote areas remains poor, as almost all companies concentrate their operations and promotions in major cities, particularly the capital Amman.

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.\(^{27}\) Citizens and businesses can obtain internet access through privately owned service providers without state approval or registration. A November 2011 report listed 16 active internet service providers (ISPs) in Jordan, though licenses have been granted to over 20 companies.\(^{28}\) The market is dominated by Umniah (a subsidiary of Batelco Bahrain), Zain, and Jordan Telecom, the local affiliate of France Telecom’s Orange brand. 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.

The TRC is the independent agency responsible for regulating the ICT sector. It is governed by the


Jordan

Telecommunications Law and defined as a “financially and administratively independent juridical personality.” 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. The TRC’s Board of Commissioners and its chairman, currently Mohammad al-Taani, are appointed by a resolution from the Council of Ministers based on a nomination from the prime minister. Nonetheless, the TRC is generally seen as independent and fair in its decision making, though it does coordinate policy with the government.

Limits on Content

This year marked an important shift in how Jordanian authorities limit online content. In June 2013, 291 news websites were blocked in the country for failing to comply with the recently amended Press and Publication Law (PPL). The law establishes limits on what websites can provide news content and reinforces economic obstacles to freedom of the press. 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 have 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.

The move to block almost 300 news sites came after the expiration of a nine-month grace period for news sites to comply with the amended PPL, passed in September 2012. The PPL places restrictions on online news editors and requires news websites to register with the government or face blocking. According to Article 49(A), any electronic publication which publishes domestic or international news, press releases, or comments is required to register with the Ministry of Commerce and Industry and acquire a license from the Ministry of Culture’s Department of Press and Publications (DPP). In
April 2014, the Director of the DPP, Fayez Shawabkeh, stated that a total of 156 websites have since become unblocked after obtaining a license.\textsuperscript{39}

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 "Any 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."\textsuperscript{40} Articles 48 and 49 enable the Director of the DPP to block any website for failing to obtain a license or, more broadly, for violating Jordanian law. In addition to facing blocking, unlicensed websites also face a potential fine of JOD 1,000–5,000 ($1,500–7,500) according to Article 48(B). The blocking occurs through a direct request from the director of the DPP to the TRC, with the TRC chairman then sending a decree to ISPs to implement the blocking. The law also requires that editors-in-chief of online outlets must have been prior members of the Jordan Press Association for a period of at least four years. The Director of the DPP estimated that Jordan contains some 400 news websites.\textsuperscript{41}

The move was met with consternation, particularly as Jordan does not have a history of extensive web filtering. For a number of years, the only blocked website was the U.S.-based Arab Times, which often takes a critical tone toward Arab regimes.\textsuperscript{42} In the past, however, authorities had failed in their attempts to impose greater restrictions on content. In 2008, authorities blocked access to about 600 websites on internal government networks, claiming such measures were necessary to prevent public service employees from wasting time online. The inclusion of key Jordanian news websites among those blocked raised concerns that the purpose was also to limit government employees' access to independent information.\textsuperscript{43} Marouf al-Bakhit, the prime minister at the time, reversed this policy in 2011.

As recent as July 2012, some groups have staged small protests and even launched a Facebook campaign to push the MoICT to block pornography sites.\textsuperscript{44} Internet freedom activists have been highly critical of any potential move, citing the potential for widespread censorship due to overblocking.\textsuperscript{45} According to one official, authorities may instead insist that ISPs offer a voluntary service to block these sites for subscribers.\textsuperscript{46} So far, there is no evidence that the ISPs are voluntarily...

\textsuperscript{42} AlBawaba, “Jordan: Lifting up the Block only on a few websites,” June 5, 2013, accessed June 26, 2013.
\textsuperscript{43} A test by Freedom House in February 2012 confirmed that the website remains inaccessible. See also, “Jordan,” OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/jordan.
\textsuperscript{45} According to one official, authorities may instead insist that ISPs offer a voluntary service to block these sites for subscribers.
blocking websites. However, the Jordanian government proposed a new Communication Law this year that would require the TRC to issue a set of instructions that force the companies licensing and operating public information to prevent access to pornographic websites and content.\textsuperscript{47} The ICT minister, Dr. Azzam Slait, reportedly withdrew the proposed law, sending it back for further consideration and possible amendments in mid-2014.\textsuperscript{48} The law was published on the Legislation and Opinion Bureau’s website to solicit feedback from the public.\textsuperscript{49}

In a more subtle censorship dynamic, website owners have occasionally acted to remove, or refrain from publishing, online content after receiving informal complaints from government officials, members of the security services, party leaders, lawmakers, journalists, and even ordinary users. Websites that refuse such requests have faced reprisals. The military court reportedly asked owners and editors-in-chief of all Jordanian news websites to refrain from publishing any news or information on issues related to the Jordanian military and its personnel, except after a “direct and clear request to the authorized military sources.”\textsuperscript{50} The request was delivered through a letter sent to the DPP. In 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.

The director of the DPP issued another brief to online media outlets, telling them to refrain from publishing further news regarding a doctor who was reportedly infected with malaria while in one of Jordan’s Dead Sea resorts, and died. The order came in response to a request by businesses in the resort area.\textsuperscript{51}

In another incident from March 2012, the Jordanian Royal Court pressured the website of the al-Arab al-Yawm newspaper to delete an article titled, “We will not live in a stupid man’s robe,” which criticized the government’s handling of corruption and protests in the city of al-Tafila.\textsuperscript{52} In other cases, news websites that tackle sensitive issues must deal with waves of angry comments from conservative readers.

Intermediaries face increasing liability for content posted to their sites. The 2012 amendments of the PPL place 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.\textsuperscript{53} Moreover, websites must keep a record of all comments for six months after initial publication and refrain from publishing any “untruthful” or


\textsuperscript{53} Law number (32) 2012. Amendments to The Press and Publications law for the Year 1998 (8).
“irrelevant” comments. Journalists in Jordan stated that the new changes in the law are intended to increase self-censorship and instigate fear among journalists. Article 38 of the PPL prohibits specified material from being published, including any “contempt, slander, or defamation of or abuse of” a religions or prophets. The same article prohibits publishing any material defamatory or slanderous of individuals who are also protected by the same law against “rumors” and “anything that hinders their personal freedom”. Furthermore, the amended PPL has forced many news sites to register with Chamber of Commerce and obtain a license from the Department of Press and Publications, thus opening themselves up to direct legal action by the government. Overall, the threat presented by restrictive laws and financial penalties in the PPL, combined with an awareness of extensive content monitoring, has a chilling effect on online speech. (See “Violations of User Rights” for a discussion on punitive laws and surveillance.)

Many bloggers and website owners 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 recent 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. Traditional journalists often start their own blogs in order to be free from editorial censorship. Since 2011, blogs have regained their importance as an avenue for debate on political and social issues. A growing number of blogs are also written in Arabic, a shift from several years ago when most were in English or bilingual.

The amended law also affects the financial viability of online news websites by prohibiting foreign investment in newspapers, a provision that could now apply to online news outlets as well. All licensed websites must pay to acquire a license to “legally” operate within the country and avoid being blocked. The Council of Ministers was assigned the task of regulating licensing and registration fees, but little information about the process has been made public. Indeed, there are reports that the DPP Director, Fayez Shawabkeh, announced that the government will not require any licensing fee. Observers believe this decision to be a tactic by the Jordanian government to release tension after the local and international outcry over the blocking in June 2013.

Meanwhile, in mid-2012, unconfirmed reports emerged of government agencies pressuring advertisers to avoid certain news websites in an effort to limit the sites’ income. There have also been some initial reports of security or government officials offering encouragement—and possibly...
material support—to journalists to establish news websites favorable to the government that would compete with the increasingly influential, and often critical, existing online outlets. Media analysts and online news editors have indicated that political candidates, for example, purchase advertising on news websites in a bid to avoid negative coverage. At the same time, the more popular news sites have benefitted from the high number of daily hits, presenting a strong alternative to advertising in traditional media. A survey by the Center for Defending Freedom of Journalists revealed that 76 percent of all journalists believe that online news websites are more prone to accepting gifts and even cash in return for favorable news reports.

Overall, the country’s hundreds of news websites are an increasingly important source of information and analysis for many Jordanians. Many feel that online sources discuss a wide range of topics typically avoided by traditional media outlets. A study released by the market research firm Ipsos in March 2012 found that around 70 percent of internet users accessed news websites, making it the most popular area of online interest, surpassing music and sports. Nine news websites—Sarayanews, Alwakeelnews, Ammonnews, Gerasanews, Garaanews, Panet, Tasweernews, Royanews, and Jfranews—were among the top 25 most visited websites in the country in mid-2014. The general perception is that online journalists tend to focus more on opinion pieces and pushing social or cultural boundaries than their counterparts in traditional media.

There is no evidence that English language websites, like the Jordan Times, are subject to similar pressure from the government or other state departments. While the Jordan Times is owned by the Jordan Press Foundation, a public company listed on the Amman Stock Exchange, the Jordanian government is one of its main shareholders.

Social media applications such as Facebook, the micro-blogging service Twitter, and the video-sharing site YouTube are very popular, particularly among younger Jordanians. There are over two million Facebook users in Jordan, representing over one-third of the country’s population, with a penetration rate of 47.9 percent of the population as of May 2014, of whom 59 percent are male. Twitter has garnered a much smaller following of around 161,000 users, or around 2.4 percent of the population. Several local social media tools, such as the Jordanian microblogging site WatWet, have shut down because they failed to compete. State officials, including the Royal Hashemite

Court, the Queen, the Crown Prince, and Prince Hassan have established social media accounts to communicate with the public. Queen Rania is by far the most popular of these accounts, with over 3 million followers on Twitter and over 200,000 on Instagram. She was, in fact, referred to by Forbes Middle East magazine as “The Queen of Social Media.” Among government officials, Foreign Minister Nasser Judeh has around 50,000 Twitter followers, while an unverified account related to Prime Minister Abdulla Ensour has 5,000 followers.

These online tools, 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. 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.” However, social media activity and numerous protests failed to halt the bill from being passed 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 garnered more than 37,800 likes as of May 2014. The government responded in 2013 by introducing a new telecommunications law that, if passed, would prohibit ISPs from allowing users to access pornographic websites under article 61.

While public demonstrations were less visible this year, in March 2014 social media helped organize demonstrations to protest the killing of the Jordanian judge Raed Zuiter by the Israeli military on the border between Jordan and the West Bank. A Facebook page was created in his memory with more than 10,000 likes.

Violations of User Rights

A host of repressive laws and severe punishments create an environment of fear in Jordan, where

---

70 http://instagram.com/rhcjo
71 http://instagram.com/ahusseinbinabdullahi
72 https://twitter.com/majliselhassan
75 See https://twitter.com/DrEnsour.
77 See Facebook.com. May 12, 2014, https://www.facebook.com/pages/%D8%A7%D9%84%D8%B1%D8%A7%D8%A6%D8%AF-%D8%82%D8%B9%D9%8A%D8%AA%D8%B1/293893970763114?sk=info.
80 See Facebook.com. May 12, 2014, https://www.facebook.com/pages/%D8%A7%D9%84%D8%B1%D8%A7%D8%A6%D8%AF-%D8%82%D8%B9%D9%8A%D8%AA%D8%B1/293893970763114?sk=info.
journalists, political activists, and ordinary users face arrest and possible prosecution if they overstep the boundaries of acceptable speech. While extralegal attacks and physical harassment of users has decreased over the past year, three citizens faced charges before the military-dominated State Security Court for their online activities over the coverage period. Strict penalties for criminal defamation against public authorities, both foreign and domestic, remain a prominent concern. At the same time, the passing of a new anti-terrorism law, as well as proposals for a new communications law, present another grave threat to internet freedom.

In October 2011, responding to public discontent, constitutional amendments were introduced to strengthen checks and balances and ensure greater protections for human rights.81 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).82 The Constitutional Court’s nine members were named by King Abdullah II in October 2012.83 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).84

Despite 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. Despite the passage of an Access to Information Law in 2007, a number of restrictions remain on requesting sensitive social and religious content.85 In September 2011, the lower house of parliament passed an amendment to the Anti-Corruption Law which would have penalized the publication or dissemination of allegations of corruption without proof with fines ranging from JOD 30,000 to JOD 60,000 (US$42,000 to US$84,000).86 However, in January 2012, the upper house of parliament rejected the controversial

85 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) Arab Archives Institute, “Summary of the Study on Access to Information Law in Jordan,” June 2005, http://www.alarcheef.com/reports/englishFiles/accessToInformation.pdf.
article following advocacy efforts by civil society groups and threats by the board of the Jordan Press Association to resign.87

Most recently, the amended Press and Publication Law bans the publishing of “material that is inconsistent with the principles of freedom, national obligation, human rights, and Arab-Islamic values.”88 Journalists, website owners, and editors-in-chief face a fine of JOD 5,000 (US$ 7,500) if found to violate Article 5 of 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).89

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.90 At the time, the changes were seen cosmetic at best, with Human Rights Watch stating that Jordan needs to “overhaul its outdated penal code and stop dragging civilians in front of the State Security Court just for demonstrating for reform.”91 Most worryingly, amendments to the anti-terrorism law passed in mid-2014 essentially reverse many of the advances made in the law by expanding the definition of “terrorism” to include offenses that do not directly relate to the causing of physical damage or violent attacks.92

The amendments to the 2006 anti-terrorism law were sanctioned by the Senate on May 1,93 and endorsed by King Abdullah II on June, 1, 2014.94 The amendments have been criticized for “broadening the definition of terrorism and threaten[ing] freedom of expression”95 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,”96 an offense that had already been listed in the penal code. The new law also covers any “use of an information system or information network or any other publication or media outlet or website to facilitate terrorist acts, to support a group, organization, or

88 Law number (32) 2012. Amendments to The Press and Publications law for the Year 1998 (8).
89 Law number (32) 2012. Amendments to The Press and Publications law for the Year 1998 (8). Article 46 (E)
society” which commits, promotes, or funds terrorist acts, or to subject “Jordanians or their property to danger of hostile acts or acts of revenge.”

Political analysts understood the new amendments in the context of the security threats posed by the proximity with Syria and the tensions growing in the region. However, many critics view the bill as a tool for the government to crackdown on the opposition and impose further restrictions on media freedom. 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 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. The law comes at a time when neighboring countries, such as Egypt, Saudi Arabia, and the United Arab Emirates, have outlawed the Muslim Brotherhood as a terrorist organization.

The 2010 cybercrime law proscribes 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.

Defamation remains a criminal offense under the penal code. Amendments to the press law enacted in 2010 abolished prison sentences for libeling 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 three to twelve months imprisonment. On April 25, 2013, Mohammad Asha al-Dawaymeh, a parliamentarian from the Islamist Centrist Party, filed a suit against the website Ammon News for publishing news about a visit to Israel he made earlier this year. He was later expelled from his political party over the visit, during which he reportedly attended a reception with Israeli President

---

Shimon Peres to celebrate Israel’s Independence Day. While a hearing was held in January 2014, there have not yet been any reports of a verdict in the defamation case.

For the most part, Jordanian authorities have not made use of these laws to sentence domestic political opponents to lengthy prison terms, though some online commentators have faced legal harassment. In September 17, 2013, the publisher of a Jordanian news outlet, Jafra, and its editor-in-chief were arrested under the penal code for publishing a third-party YouTube video that was thought to be offensive to Crown Prince Jassim Bin Hamad AlThani of Qatar. Amjad Mu’ala and Nidhal Farachinery were investigated and detained. The journalists were “charged with carrying out acts that the government does not approve and that would expose Jordan and its citizens to the risk of acts of aggression,” a court official reportedly said. The two were to be tried in front of a military court and faced two- to five-year prison terms. The military court repeatedly rejected requests to free the two journalists on bail, despite numerous calls from human rights organizations.

Two sit-ins were organized by the Jordanian Press Association (JPA) in solidarity with the journalists and requesting their release on December 24-25, 2013, with the JPA Council threatening to resign two days later. On December 31, an appeals court ruled to release the two individuals on bail for JOD 3,000 (US$ 4,000) and the case was transferred to the Amman Court of First Instance, a civilian court.

This was not the only case of online journalism professionals being charged over the coverage period. Hashem Khalidi, publisher of the Saraya News website, was accused of lacking attention to accuracy, publishing false news, and publishing materials offensive to individuals. Two lawsuits were filed against the publisher on November 4, 2013, by a former minister of education and a former member of parliament.

In October 2013, Ayman al-Bahrawi was accused of “lengthening the tongue” and “insulting” foreign heads of state in private messages found on the Whatsapp messaging application on his mobile phone. His lawyer reported in AsSabeel, a Jordanian daily newspaper, that al-Bahrawi faced these charges before the State Security Court. According to his lawyer, al-Bahrawi’s was also accused of a

110 France 24 ‘Jordanian authorities arrest two journalists after publishing a Youtube Video that was seen as a sexual scandal for a Qatari Emir,” September 18, 2013, http://f24.my/1ycbfqA.
second charge of committing actions that can disturb relations with Arab countries.\textsuperscript{118} News reports also mentioned a separate charge of “lengthening the tongue” for messages that criticized the king.\textsuperscript{119} One of the news sources stated the message to be “It turned out that El-Sisi is worse than Bashar [reference to Syrian President Bashar al-Assad]. Damn them both”.\textsuperscript{120} Al-Bahrawi’s lawyer had asked for Jordanian Foreign Minister Nasser Judeh and the Egyptian Ambassador to Jordan to testify whether the relation between the two countries (Egypt and Jordan) was negatively affected by the messages.\textsuperscript{121} The request was rejected by the military court in March. Al-Bahrawi and his associates were finally released on bail on December 25, 2013, one day after they announced their intentions to commence a hunger strike. They were released for US$ 1,500 each and a hearing was scheduled for later in 2014.\textsuperscript{122} Importantly, the accusations faced by al-Bahrawi, Mu’ala and Fara’neh have now been incorporated into the new anti-terrorism law, passed in April 2014.

The al-Bahrawi trial is indicative of state surveillance of private communications, since the content for which he was tried was communicated to a group from 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.”\textsuperscript{123}

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.\textsuperscript{124} Authorities claim these restrictions are needed 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.

Over the past year, incidents of physical harassment and cyberattacks against bloggers and staff of online news websites have decreased in severity. Jordanian policemen targeted journalists with teargas during protests in Amman in November 2012.\textsuperscript{125} Unknown perpetrators raided the offices of

\begin{thebibliography}{9}
\bibitem{120} Amman, “Jordan: Cynical Remarks after the trial of an activist for Lengthening the Tongue,” October 1, 2013, \url{http://amman1.net/jonews/herak-heart/50048.html}.
\bibitem{125} Talhouk (2012).
\end{thebibliography}
Jordan

the online news site *Watan* on July 17, 2012, stealing documents and damaging equipment.126 The webpage of the news sites *Khaberni* and *Al Ain* were hacked in March and October 2012 respectively, while the site of the Jordanian rap group Ahat was also hacked on September 15, 2012.127 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.128

---


Kazakhstan

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partly Free</td>
<td></td>
<td></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>23</td>
<td>23</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>59</td>
<td>60</td>
</tr>
</tbody>
</table>

Population: 17 million

Internet Penetration 2013: 54 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

* 0=most free, 100=least free

Key Developments: May 2013 – May 2014

- The decree on “Rules for the Application of Additional Measures and Temporary Restrictions during a State of Emergency," which was adopted on January 28 and went into effect on April 12, 2014, allows authorities to suspend or terminate media publications and requires media outlets to provide copies of material for approval prior to publication during a declared state of emergency (see Obstacles to Access and Limits on Content).

- On April 23, 2014, the president signed amendments to the communications law that allow the authorities to block websites or shut off communication networks without a court order (see Obstacles to Access and Limits on Content).

- In May 2013, President Nursultan Nazarbayev signed the law “On personal information and its protection" under which investigative reporters can now be charged with violating the privacy of public officials if they publish information about corruption (see Violations of User Rights).
Introduction

The government of Kazakhstan has passed multiple laws or decrees over the past year that, if applied, would significantly inhibit media and internet freedoms. On April 12, 2014, a restrictive “state of emergency” decree went into effect that would allow authorities to suspend or censor media outlets during a declared state of emergency, including political or social crises such as mass riots. Further, on April 23, the president signed amendments to the communications law allowing the authorities to shut off communications networks or block websites in the event of calls for mass public actions or unrest, or incitement to take part in extremist activities. These new regulations have the potential to significantly curb freedom of expression and press freedoms in the country, though as of May 2014, they have yet to be applied to restrict online media.

Since the late 2000s, Kazakhstan’s officials have been declaring information and communication technologies (ICTs) a development priority, including at a number of international conferences and exhibitions hosted by the relevant state bodies. In the last couple of years, however, they have been comparatively quiet on the issue, reflecting both the government’s shift to a new “pet topic” (green economy, the main theme of the World Expo 2017 to be held in Astana), and its heightened cautiousness regarding the potential threats of online communications as the autocracy approaches an uneasy transition period, with the incumbent president aging.

The ministry of transport and communications, together with Kazakhtelecom, the main telephone and internet access provider, continue efforts to upgrade the country’s ICT infrastructure and to improve and promote e-government services. State entities have been instructed to enhance their websites to incorporate better feedback functionality and to set up official accounts on social networks. The e-government portal offers citizens an opportunity to file inquiries with the responsible state bodies using a personal digital signature, though officials may often decline service, referring to technical problems. In a declared attempt to promote transparency, the website for government procurement tenders was launched in July 2012; however, the potential for public oversight is restricted since only businesses competing for contracts can gain access to documentation. It was also stated that a separate OpenData portal will be developed, but there is no precise vision for it so far (currently, it contains only scattered reference data; Kazakhstan is not a member of the Open Government Initiative). Competition exists between internet service providers (ISPs), though it is limited by the national operator Kazakhtelecom’s dominance in the market, especially of wired connections. Mobile operators, on the other hand, actively compete for subscribers.

In the past few years, critical media outlets have been blocked, including the website of the banned Respublika newspaper and NurAdam.kz, the website of the Adam opposition magazine. Additionally, sites such as Ratel.kz, the online project launched in 2013 by a group of prominent journalists, have suffered from DDoS attacks, even though hard copies of their small circulations could easily be found in the newstands of Almaty. Most cases of prosecution of individuals involving the internet have been rooted in the individuals’ offline activism, rather than caused by their online activity.

The authorities clearly fear the internet’s democratizing potential, which has led the government to pass legislation to acquire broader control over the internet, often disguised as national security or anti-terrorism amendments, in addition to the legally endorsed practice of blocking certain websites. In May 2013, President Nursultan Nazarbayev signed the law “On personal information
and its protection,” which was criticized by media activists as restrictive for journalism.\(^1\) According to observers, investigative reporters can now find themselves under threat of criminal defamation charges if they publish information about official corruption that is incorrect, or, if the information turns out to be true, they can still be prosecuted for violating privacy rights. In July 2013, another law was passed that doubled the prison term for fomenting riots or “active noncompliance with lawful orders of power representatives.”\(^2\) Additionally, in October 2013, the Prosecutor General’s office announced that the country’s new criminal code would feature harsher punishment for “cybercrimes,” including the spread of “socially dangerous, destructive materials,” and for insults or libel on the internet.\(^3\) The discussion on the draft code was still in progress in the Kazakhstani parliament as of the end of this report’s coverage period.\(^4\)

### Obstacles to Access

Internet access has grown significantly in Kazakhstan, increasing from a penetration rate of 11 percent in 2008 to 54 percent in 2013, according to the International Telecommunication Union (ITU).\(^5\) Official statistics consistently inflate this indicator, and experts often question these figures, citing a lack of clarity in the methodology.\(^6\) In 2013, the ministry of information and culture declared that nearly 10 million Kazakhstanis use the internet (over 62 percent of the total population),\(^7\) or nearly all citizens between the ages of 16 and 62.\(^8\) The independent think tank Profit Online argues that this figure might count the number of devices that connect to the internet in a one month period, whereas the number of monthly internet users would be around 50 percent, while the core usage (users accessing the internet at least several days a week) would be formed by a pool of 2.5 million Kazakhstanis, around 16 percent of the total population.\(^9\)

Despite these statistical discrepancies, the trends clearly indicate a pattern of growth, although it has slowed over the past few years, even when judged by official declarations (in 2012 the figure claimed by the government was 60 percent). More people prefer to access the internet from home, alongside widening free access at educational institutions, workplaces, and public places. Internet speeds offered by the national operator Kazakhtelecom and private ISPs have increased at a slow but steady pace. Prices remain relatively expensive for the majority of the population, but both Kazakhtelecom and the ministry of transport and communication continue working together to decrease connection and usage fees. Prices have been lowered on wholesale web traffic for smaller

---

2. "Nazarbayev signed the law that doubles prison terms for inciting unrest in Kazakhstan,” Zonakz.net, July 4, 2013, [http://zonakz.net/articles/70453](http://zonakz.net/articles/70453)
4. The president signed the criminal code outside of this report's coverage period, in July 2014.
ISPs, and retail prices for users were lowered in rural areas by 20 percent for Super-EVDO and 35 percent for CDMA-EVDO technology, with prepaid traffic of 3 GB to 7 GB depending on the tariff. In late 2013, Kazakhtelecom continued investing in upgrades of its infrastructure, launching the largest internet data center in the Commonwealth of Independent States (CIS), and a 100 Gbps channel that is meant to improve consumption of external traffic.

Kazakhtelecom's unlimited broadband subscriptions currently cost US$25 to $30 per month for 20 and 30 Mbps, respectively, while basic contracts offer 3GB to 10GB of high-speed traffic for a fee of US$12 to $20 with no extra charge for exceeded traffic, which is provided at a slower speed. These prices are relatively expensive when compared to the average monthly income of approximately US$700 as of November 2013. Kazakhtelecom's main competitor, Beeline, offers similar prices for unlimited contracts, but connectivity speeds are higher while prices for basic contracts are 30 percent cheaper. The number of fixed (wired) broadband subscriptions reached approximately 12 percent of inhabitants in 2013, according to estimates from the ITU.

Mobile phone penetration is significantly higher than internet usage, with a penetration rate of over 180 percent in 2013. Mobile telecom operators increasingly compete on the market of internet access both with each other and with other ISPs since the launch of 3G in late 2010. A growing number of people are accessing the internet on their mobile phones, tablet computers, or regular computers with USB modems. In December 2012, ALTEL, a Kazakhtelecom subsidiary, launched a 4G LTE network that is currently available in six oblasts, covering 30 percent of the total population.

Since 2009, WiMAX has become available in Kazakhstan, mostly enjoyed by corporate clientele. In 2012, the major mobile operator Kcell, a subsidiary of the Scandinavian TeliaSonera, acquired WiMAX networks in six regions of Kazakhstan from the local company Alem Communications, sparking rumors that the spectrum would be used to develop LTE technology. In March 2013, another asset of Alem Communications—Digital TV, a cable television and internet operator—was purchased by Kazakhtelecom, which is also a significant IPTV provider in Kazakhstan.

The number of free Wi-Fi hotspots in public places has been growing, while internet cafes have experienced a decline in their customer base, especially in larger cities. Multiple respondents from different regions of Kazakhstan testify to the fact that cybercafes do not play a significant role as

---

access points, with most people preferring to use the internet via mobile devices and free Wi-Fi hotspots in cafes and public places, which are not subject to any government regulation. Following government instructions, Kazakhtelecom has set up public hotspot terminals for free public access to e-government services and websites in state agencies, airports, and libraries.

Kazakhstan’s “.kz” top-level domain was introduced in 1994. Currently there are more than 98,700 domains registered under “.kz” and over 1,500 domains registered under the Cyrillic “қаз” domain (introduced in 2012), although only 62 percent and 30 percent of them are active, respectively, and even fewer receive at least 100 visitors per day. The government has initiated several programs to stimulate internet use, lower the digital divide, and expand e-government services. Payments (fees and dues for state services, fines, taxes, utilities, etc.) through Egov.kz reached US$6.5 million in 2013, while new state services are continuously added, and the portal’s mobile applications are being further developed.

Social-networking platforms and other online communication apps are increasingly popular in Kazakhstan. In the late 2000s, the government invested substantial funding into creating local analogs of popular social networks, but only the video archive Kaztube.kz survived (although its user-generated content has diminished), while others failed to generate any worthwhile user base.

The most-accessed online resources from Kazakhstan are foreign, especially Russian-based social-networking sites like Mail.ru, VKontakte.com and Odnoklassniki.ru, multiservice portals like Google and Yandex, and other sites such as YouTube, Facebook, and Wikipedia. The most-visited Kazakh site as of January 2014 was the automobile-related classified ads site Kolesa.kz, followed by the online marketplace Slando.kz, which were ranked at 12th and 13th place, respectively, out of all sites accessed within the country.

In January 2012, amendments to the Law on National Security enabled the government to forcibly suspend telecommunications during counterterrorist operations or the suppression of mass riots (Article 23.4), although the government has not resorted to such methods since then. Also in 2012, new legislation governing intellectual property rights was adopted to criminalize the illegal use of copyrighted material (punishable by one year in prison) and the organized distribution of such material through a file-sharing hub (punishable by five years in prison). Since then, all

---

Kazakhstan

Kazakh torrent tracking websites have re-registered their URLs outside of the “.kz” domain zone. Additionally, content providers have started seeking ways to offer legal, licensed music and videos.

The state (through the Sovereign Wealth Fund “Samruk-Kazyna”) owns 51 percent of Kazakhtelecom, the largest ISP, which holds an 88 percent share in the broadband internet market. Independent ICT experts refute the allegation that other backbone operators are required to channel at least part of their traffic through Kazakhtelecom's network infrastructure, arguing that they might rent the national operator’s network (the most developed one) for economic reasons. Among the five backbone ISPs, only one—Beeline—is not controlled by the government (others are affiliated either with Kazakhtelecom or other national companies, and one ISP—initially a state-owned petroleum company's subsidiary—has unclear ownership status).

The Traffic Exchange Point—a peering center, established by Kazakhtelecom in 2008—is meant to facilitate service of first-tier providers, but in 2010, it turned down Beeline's application to join the pool without giving any reason. Kazakhtelecom's dominance over the market and data transfer routes creates conditions for systemic content filtering.

The government's decree on the rules of interaction and centralized management of telecommunication networks, dated December 8, 2011, regulates the activities of all ICT operators and aims—among other tasks—to “collect and analyze data about the current condition of traffic on international communication lines” and “provide for the court or investigatory bodies’ decisions on the suspension of operation of any networks or means of communication.” Once the relevant state technical service receives the official decision on suspension, it immediately turns it into action and informs telecom operators on the technological parameters of the procedure. In order to provide for state supervision over the execution of such a decision, telecom operators must grant physical access to its own network control center.

On February 13, 2014, two days after an abrupt currency devaluation that frustrated many citizens, a call to hold an unsanctioned rally in Almaty became viral via its dissemination through SMS and mobile applications. At around 5 p.m., users of all mobile operators in Almaty reported problems with WhatsApp, Viber, and SMS services, which were unavailable for nearly 1.5 hours. Operators either refused to comment or cited “reasons not related to the company” for the problem. Aside from this temporary disruption, there have been no instances of major disruptions in connectivity during the coverage period, but many proxy sites used as circumvention tools are blocked.

29 Interviews (January 13, 2014).
31 See full text of the Rules here http://adilet.zan.kz/ru/docs/P1100001499
On January 1, 2014, the website Ratel.kz posted a presentation by the ministry of communication and information (presumably, dated between December 16, 2011, when the events described in the presentation took place, and January 14, 2012, when the ministry was reorganized) regarding the government’s brutal suppression of an oil worker strike in Western Kazakhstan that turned into mass riots and became known as the Zhanaozen crisis.\(^{33}\) The presentation suggests that the government then disrupted all communications in the town (it was officially stated that the telecom lines were hit by fire) and continually blocked websites publishing unwanted information.\(^{34}\)

On April 23, 2014, the government further expanded its legal authority to shut down ICTs when the president signed the law “On amendments and addenda to laws governing activity of the internal affairs bodies,” which grants the prosecutor general’s office the authority to suspend the operations of communication networks, including the provision of communication services and access to websites or particular content on websites, without a court decision. This law applies to cases when the networks are used for “felonious aims to damage the interests of individuals, society or state,” including the dissemination of illegal information, calling for extremism, terrorism, mass riots, or participation in unauthorized mass public gatherings. Temporary bans can be introduced by the prosecutor general and deputy prosecutor general, whose instruction is then sent to the relevant authority. Within one hour, the relevant authority must inform service providers of the decision, which must be implemented within three hours. The law also provides for the deletion of disputed content by the person responsible for posting it online. If the publisher complies, the website can then be unblocked.\(^{35}\)

As of April 2013, there were four mobile telephone providers in Kazakhstan, three of which use the GSM/3G standard (Kcell, Beeline, and TELE2) and one that uses CDMA/4G (ALTEL). Currently, all GSM operators are privately owned, with large foreign participation in ownership. Kazakhtelecom has fully owned ALTEL since 2006.

Several bodies regulate the ICT sector, with the main regulators reorganized periodically. In January 2012, the ministry of transport and communications was given responsibility over the technology infrastructure sector, while regulation of information-related issues was entrusted to the Committee for Information and Archives at the ministry of culture and information. In March 2014, the president issued a decree forming a separate agency known as the Agency for Communication and Information to manage issues of communication, information, and archives. There is no independent body holding a regulatory mandate to oversee internet. The Internet Association of Kazakhstan, established in 2009 in the form of a union of legal entities, claims to unite the Kazakh internet community to “improve infrastructure for Kazakhstan segment of the World Wide Web, develop common rules and reveal problems of the industry.”\(^{36}\) It participated in several working groups on internet-related legislation, yet some experts and professionals in the field have questioned the group’s independence, transparency, and non-profit status.\(^{37}\) The association does not have an


official government mandate but aims to “represent the interests of Kazakhstani internet market in state bodies” and has signed a memorandum of cooperation with the Prosecutor General’s office on “fighting illegal content.”

The “.kz” top-level domain is managed by a registry, the Kazakhstani Network Information Center (KazNIC), and the Kazakhstani Association of IT Companies. Both were created in 2004–2005 as formally nongovernmental organizations, but in practice, they are believed to be under close control of the authorities and have been known to make politicized decisions on registration and deregistration of domain names. 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**

In 2014, two laws were signed that grant greater authority to the prosecutor general and local government officials to block or censor online content. In addition to authorizing the suspension of ICT networks, the law “On amendments and addenda to laws governing activity of the internal affairs bodies,” signed by the president on April 23, 2014, grants the prosecutor general’s office the authority to block websites, without a court decision, if the websites are found to host illegal content. Additionally, the decree on “Rules for the Application of Additional Measures and Temporary Restrictions during a State of Emergency,” which was adopted on January 28 and implemented on April 12, 2014, allows officials to suspend or terminate media outlets and requires media outlets to provide local authorities with copies of material prior to publication during a declared state of emergency.

According to Adil Soz, a media rights NGO in Kazakhstan, there were 11 cases of media suspensions or forced closures in 2013, including of online media outlets, most of which were voices of the opposition or those that were critical of the government. They also reported on 14 cases of continuous or temporary website blockings, including the short-term outage of Facebook, reported by users in three cities.

In 2009, the country’s media legislation was amended to require a court decision to block a website. In addition, court approval is legally required for any filtering to be exercised by ISPs according to the 2009 amendments to the ICT regulation. However, these requirements have been inconsistently followed. The courts generally issue decisions to block websites in a frequent and dense manner, banning dozens of websites 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. The authorities have also sought to undermine the effectiveness of circumvention tools.

The legal framework for blocking online content changed following the amendments made on April 23, 2014 to the law, “On amendments and addenda to legislation regarding work of bodies of internal affairs,” most of which were related to internet resources and their blocking. In addition to granting the prosecutor general’s office the authority to suspend the operations of communication networks (as discussed above in “Obstacles to Access”), the new regulation provides for the suspension of access to websites without a court order, following the prosecutor general’s request sent to the telecom providers or State Technical Authority by the Communications and Information Agency. However, after the owner of a resource removes the disputed content to comply with the request, the law demands access to be restored. This legislation runs counter to the law “On mass media,” which still requires a court order to suspend or close access to websites.

Additionally, the decree on “Rules for the Application of Additional Measures and Temporary Restrictions during a State of Emergency,” which was adopted on January 28 and entered into effect on April 12, 2014, imposes a number of restrictions to freedom of expression and association. According to this law, Kazakh authorities can act with minimal judicial oversight, issue orders to suspend or terminate media publications (including on the internet), and suspend the activities of political parties and public associations during a state of emergency. Also during this time, media agencies must provide copies of material for publication to the local authorities at least 24 hours in advance, or in the case of breaking new reports, immediately before publication, in order to “align its content.” If the outlet publishes any information that has not been approved, the commandant can issue “an order to suspend for a period established by law and/or to terminate production of mass media materials, or stop the distribution of mass media reports.” These new regulations have the potential to significantly infringe on internet users’ rights and the principles of press freedom, although as of May 2014 they have yet to be applied.

Social media sites have been periodically blocked in Kazakhstan in recent years, though the government has not always admitted intent behind the restrictions. The international blog-hosting platform LiveJournal was blocked for over two years from October 2008 to November 2010 by Kazakhtelecom, ostensibly to restrict access to politically-sensitive content related to President Nazarbayev’s former son-in-law, Rakhat Aliyev. The platform was unblocked after the disputed blog

47 Rakhat Aliyev, Nazarbayev’s former son-in-law, had served in top positions in the country’s secret services and diplomatic service. He had large business and media holdings before definitively falling out of favor with the president and his family in 2008 after he had faced multiple charges of abduction, financial crimes and a coup attempt. Having fled abroad, Aliyev began airing inside information and allegations, in the traditional media and online, in an effort to discredit the president. Materials related to Aliyev have been systematically filtered, and republication of excerpts from his book “Godfather-in-law” is officially banned. Many observers believe that Nazarbayev’s conflict with Aliyev was the primary reason for the first blockage of LiveJournal in Kazakhstan, and also accelerated adoption of the internet-related legal amendments in 2009.
Kazakhstan

was frozen by LiveJournal administrators, yet blocked again in August 2011 under claims that some accounts contained religious extremism. A LiveJournal spokesperson stated that the company had never received any official notice from the Kazakhstan government identifying certain accounts as extremist and requesting their removal, an action the blog-hosting provider claimed it would take if the concerns were found to be legitimate. The site remained inaccessible from Kazakhstan during this report’s coverage period.

In February 2011, a district court in Astana banned two blogs on the Wordpress platform for disseminating content related to religious extremism, but this resulted in the blocking of the entire platform. It is not fully clear when access was restored, and the disputed blogs are no longer available. As of 2014, Kazakhstani users can access Wordpress.com. Users reported the inaccessibility of some web-based services, including Slideshare.net, which was returning a “408 Request Time-out” error message in fall 2013. The live video streaming site Bambuser.com was originally blocked in April 2012 and remains inaccessible.

In 2011–2012, Kazakhtelecom users had persistently reported difficulties in accessing some of Google’s services, including the ability to download attachments sent in Gmail, the Picasa image bank, Google Translate’s URL translation function, and others. The cause of the problem was unclear and was never specifically explained by Kazakhtelecom officials, although the problem ceased to exist in September 2012, reportedly after Google started using local servers to cache webpages and thus enhance its search services. According to Google’s latest Transparency Report from January through June 2013, there were 3 requests from the government of Kazakhstan (none of them supported by relevant court decisions) to delete content from YouTube, including 200 items on the grounds of national security, 8 related to hate speech, and 1 related to violence. Of the three requests (totaling 209 items requested to be removed), Google complied with some or all of two of the requests.

There were no details provided about each of the requests, but one prominent case is the blocking of a site for the Society to Assist Car Owners, an online community that is fighting against corruption and extortion of bribes by traffic police. The Society’s website was blocked at least once for several days in April 2013, supposedly because of some embedded YouTube clips that were disputed. As of

51 Svetlana Glushkova, “Портал Wordress заблокировали из-за двух блогов” [Wordpress portal was closed because of two blogs], Azattyq.org, July 12, 2011, http://rus.azattyq.org/content/worldpress_kazakhtelecom_blocking_blog_/24262786.html.
53 See Google Help forum thread (in Russian) at https://groups.google.com/a/googleproductforums.com/forum/#category-topic/gmail-ru/?????-%D0%BE%D1%80%D0%B5%D0%BC%D0%BE%D1%81%D1%82%D1%8C%D1%88%D0%BA%D0%B0/24262786.html, accessed January 31, 2013.
May 2014 the website is accessible, but its YouTube page was terminated because of "multiple third-party notifications of copyright infringement."\(^{57}\)

A package of legislative amendments adopted in July 2009, which received significant domestic and international criticism, granted the state broad authority to block access to foreign online resources whose content is deemed to run counter to national laws. The decision can be made in absentia of the website representative and requires no further notification—to the public or the website owner—about why the website is blocked. The law considers all internet resources as media outlets. Under these amendments, all ISPs are required to ensure blockage of banned websites, and the owners of "internet resources" are responsible for any content, posted either by themselves or other users, that is deemed illegal under Kazakhstan’s civil, criminal, or administrative laws.\(^{58}\)

For some time, the 2009 legal amendments stood unimplemented, but after a series of suicide bombings in 2011, several court decisions were issued ordering the blocking of 125 websites for reasons of "religious extremism."\(^{59}\) In November 2012, the National Security Committee stated that courts had banned access to nearly 950 websites in 2011–2012 for propaganda relating to terrorism, violence, and extremism, and over 150 more sites were undergoing court examinations.\(^{60}\) In addition, the filtering of opposition websites continues without court decisions.

Avaaz.org, the international platform for online petitions, became very popular in Kazakhstan after a December 2013 scandal involving a car accident in which a high-ranking official’s son had killed one and injured five in Almaty, but was released soon after his arrest. A petition to bring him to justice generated over 5,000 signatures on Avaaz.org in the first day, and this number tripled in the following two days.\(^{61}\) Another petition on Avaaz.org appeared on February 12—after the national currency devaluation—that listed recent failures of the government and urged president Nazarbayev to resign. The petition collected 2,000 signatures in the first day, after which the website was blocked.\(^{62}\) It was still inaccessible as of end of May 2014. The ministry of transport and communication, responding to the official request, said it did not order the block. Kazakhtelecom refused to comment.

Ratel.kz, a new whistleblowing site, was launched in December of 2013, and in its first two months, it survived several hacking attempts, DDoS attacks, and troubles with the hosting provider that allegedly impeded access to the website, as its founders stated at a February 18 press conference.\(^{63}\) Claiming that they were targeted because of their critical articles, the owners of Ratel denounced the

\(^{57}\) See the disclaimer here: [http://www.youtube.com/user/OCAKazakhstan](http://www.youtube.com/user/OCAKazakhstan)


\(^{62}\) "Website with the petition on Nazarbayev’s ‘impeachment’ blocked", Azattyq.org, January 13, [http://rus.azattyq.org/content/petica-onlain-otstavka-nazarbaeva25262258.html](http://rus.azattyq.org/content/petica-onlain-otstavka-nazarbaeva25262258.html)

Kazakhstan

blocking of their website, which has been intermittently exercised by Kazakhtelecom since February 14 (Ratel has since moved to the non-Kazakh domain .su) The Ratel staff presented results of ping tracing, which showed the block stemming from one of Kazakhtelecom’s backbone facilities, and is based on a domain name rather than an IP address. The national operator denies any problems on its side.

The West Kazakhstan "Uralsk Week" newspaper’s website (Uralskweek.kz) was blocked on April 15, 2014, as reported by editor-in-chief Lukpan Akhmedyarov on Twitter.

The independent publication has faced numerous suits and administrative pressure in the past, and Mr. Akhmedyarov suffered a brutal attack in 2012. Internet users immediately launched a campaign in support of the news outlet, posting screenshots on social media of the error message that their browsers returned of the newspaper’s URL. Kazakhtelecom denied blocking the website, and access to the website was restored after one day.

As many as 596 “destructive” websites were blocked by court decisions in Kazakhstan on extremism and terrorism charges in 2013.

In January 2014, the prosecutor general’s office made an announcement that they would “master new approaches to fighting cyber-terrorism,” as currently the “reaction of state bodies to its challenges is not always adequate, due to lack of specialists.”

One of the ways to do so, according to the spokesperson, is to “collect information” instead of “mechanic deletion” of content from the web.

In March 2010, the Computer Emergency Response Team (CERT) was established in Kazakhstan to operate under the ministry of transport communications with the aim of fighting “destructive content” and “political extremism” by blacklisting and banning certain sites, but currently, the agency’s web page defines its mandate as addressing only technical incidents (viruses, spam, unauthorized access, DDoS or hacker attacks, etc.), not dealing with “issues of law enforcement authorities’ responsibility.”

In late 2012, a court order banned four of the main opposition media outlets for alleged “propaganda of violent overthrow of government and undermining of state security” in their content.

In 2012, the website of the online newspaper Guljan.org was charged with libel by state officials and eventually banned by a court with the defendants and their representatives in absentia.

In 2013, the journalistic collective reunited and registered a print magazine and website, Nuradam.

64 Twitter status of Lukpan Ahmdyrov@LukichLukpan, April 15, 2014, https://twitter.com/lukichlukpan/status/455977027099971585?refsrc=email
70 “Прокуратура Алматы просит суд закрыть ряд оппозиционных СМИ” ["Prosecutors ask court to ban several opposition media outlets"], Tengrinews.kz, November 21, 2012, http://m.tengrinews.kz/ru/kazakhstan_news/223826
71 “Гульжан Ергалиева: Я еще не знаю, в чем меня обвиняют” [Guljan Ergaliyeva: I don’t know what are the charges they bring against me], December 5, 2012, http://forbes.kz/massmedia/guljan_ergalieva_ya_esche_ne_znayu_v_chem_menya_obvinayut
Kazakhstan

kz, which suffered from DDoS attacks on several occasions. In May 2013, the chief editor of the publication Gulzhan Yergaliyeva filed a complaint with the ministry of transport and communication for illegal blocking of Nuradam.kz.72 In June, the journalists received an official reply saying that neither the ministry nor Kazakhtelecom were blocking the website.73 As of April 2014, the domain name was reregistered and now represents an online shop.

The general atmosphere of self-censorship in both traditional and online media solidified after the package of amendments passed in 2009 increased censorship of content related to national security, copyright, privacy, extra protection of the president’s honor and dignity, etc., in turn influencing the content on news sites, user-generated content platforms, and web-hosting companies. In some cases, the government suggests specific content that should not be covered in the media. For example, in December 2013, the ministry of culture and information issued an “insistent recommendation” to the media not to report on the press briefing by opposition figures about new details in the case of the opposition leader’s murder in 2006; however, several traditional and online media outlets still covered the event. No new methods were used by the government or non-state actors to proactively manipulate the content and online news landscape during the coverage period, though the presence of government-paid commentators continued to be observed.

In an effort to demonstrate a willingness to engage with citizens online, officials and government institutions continue setting up and maintaining blogs on popular social-networking platforms. The website of every government body and local administration is required to have a blog, and all government press secretaries have been advised to set up their own Twitter accounts “to regularly monitor and participate in discussions, and resolve issues right where they occur.”74

In February 2013, the minister of culture and information, Mukhtar Kul-Mukhammed, stated that future government procurement contracts with the media would favor more web-based publications for the “promotion of information policy.”75 At approximately the same time, then-state secretary Marat Tazhin expressed the need for a new information policy that would create a database of popular domestic and foreign analysts, bloggers, and moderators of social network communities.76 There have been no official reports on the outcomes of these initiatives, but media NGOs have criticized the state contracts that will reportedly reach a record of US$250 million in 2014,77 both for their propagandistic bias and lack of transparency.78 Kazbek Beisebaev, who has a prominent Facebook account, described his interaction with the Internet Association of Kazakhstan (which he identified as a “Tazhin list” operator, based on their self-presentation in private conversation)

75 “Distribution of state information procurement contracts will be strictly tied to the rating of media outlets”, Kazinform, February 25, 2013, http://inform.kz/rus/article/2537802.
Kazakhstan

as unsuccessful due to a lack of transparency in the selection of contractors and generally unclear procedures.\(^79\)

In 2013, Yvision.kz—the most popular Kazakhstan-based blogging platform, with over 120,000 registered users posting on average 100 items daily—began taking information procurement contracts from the government for promoting an e-government portal and holding a blogger conference. More websites, which were initially launched as blogging platforms, have been increasingly trying to reposition themselves as editorially-supervised publications—partly because many users are migrating to Twitter and Facebook (the latter currently has over 700,000 users from Kazakhstan by estimates of InternetWorldStats.com)\(^80\) and partly in an effort to look more like professional media outlets both for advertisers and the government’s information procurement contracts.

The Kazakhstani blogosphere experiences a wider engagement of professionals, officials, politicians, academics, and other public figures, particularly on social networks, which still remain a more open ground for discourse than traditional media outlets. The authorities have continued recruiting or encouraging some of the popular and loyal bloggers to engage in “special coverage” propaganda campaigns.\(^81\)

Several grassroots campaigns emerged in early 2013 that actively employed various kinds of social media platforms to reach out to potential supporters, spread their message, and coordinate activities. In February 2014, after a largely unexpected 20 percent devaluation of the tenge, the national currency, frustrated citizens actively shared their reactions online, and two rallies held in Almaty were coordinated mostly via Facebook and WhatsApp.

More substantial online campaigns included the “Protect Kok-Zhailau!” group, which opposed the plans of large-scale construction on the territory of a nature reserve, and a movement that opposed budget cuts to maternity benefits and an increase of the retirement age. Both groups developed consolidated positions and put forth constructive suggestions to mitigate the disputes, enabling them to resonate widely with the public, Though the campaigns garnered a limited response from the authorities, in June 2013, Serik Abdenov, the minister of labor and social protection, was fired on direct orders from the president as a result of the growing discontent around the retirement issue.\(^82\) These cases demonstrated serious self-organizing potential that was not previously present in the online sphere in Kazakhstan.

Violations of User Rights

During the coverage period, the government of Kazakhstan continued to use legal and extralegal mechanisms to control the activities of internet users. Restrictions on the use of anonymizing tools remain in place, and the government admitted to wide-scale monitoring of the web as well


\(^{81}\) “Усилились постжанаозенские баталии блогеров” [“Post-Zhanaozen battles between bloggers have intensified”], Azattyq.org, August 20, 2012, http://rus.azattyq.org/content/twitter-bloggers-battle-about-zhanaozen-trial/24680408.html

Kazakhstan

as the use of more advanced filtering technologies in fall 2013. On March 14, 2013, human rights activist and journalist Alexander Kharlamov was arrested for allegedly “spreading atheist ideas” and “inciting hatred” online, but observers believe his anti-corruption activism was the real reason for his arrest. He was sentenced to six months pre-trial detention (some of which was forcibly spent in a psychiatric ward) and now faces a prison sentence of up to seven years.

The constitution of Kazakhstan guarantees freedom of the press, but the criminal code provides stricter punishment for libel or insult of state officials, members of parliament, and especially, the president. 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 libel to punish critical reporting.

In January 2014, a new draft criminal code was sent to the parliament and underwent the lower chamber’s approval in the first reading. A separate section covers cybercrimes, including unsanctioned access to or illegal interception, modification, and deletion of information on computer networks. The new draft code makes the punishment for insult and libel – including those made in comments on websites – harsher (larger fines and up to three years of imprisonment), despite the government’s earlier commitment to decriminalize defamation. It also introduces criminal liability of up to 10 years in jail for the “dissemination of deliberately false information” and criminalizes 58 delicts that are currently covered by the code of administrative offences, most of which are related to “disturbing public order.” The new criminal code was not adopted during this report’s coverage period, which ended May 31, 2014 (the new criminal code was approved by the parliament on June 11 and was signed by the president on July 3, 2014).

In May 2013, President Nursultan 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 can now find themselves under the threat of prosecution for violation of privacy charges if they publish information about official corruption.

Kazakhstan media law considers websites as media outlets, but the practice of granting these outlets the same rights and protections as traditional media is selective. In 2013, journalist Irina Mednikova reported that government officials refused to provide her with information she requested for an article that she was writing for the website Blogbasta.kz. The officials cited the absence of the website’s official registration as a media outlet as the reason for not giving the information; however, the same law stipulates that it is not necessary for the websites to obtain such registration. In addition, new rules for the accreditation of journalists at state bodies and public associations were

83 "Appeal by the media NGOs regarding the anti-constitutional amendments introduced by the Office of General Prosecutor", April 7, 2014, http://t.co/wESn7DKzp .
adopted by the ministry of culture and information on June 21, 2013. These rules make it impossible for online media outlets without official registration to obtain such accreditation.\textsuperscript{87}

The first case of online libel in Kazakhstan reached the courts in January 2013. Two officers of the Almaty tax department published an anonymous post on the official blog of the chairman of the tax committee, claiming that their supervisor was implicated in crimes of corruption. The police inquired into the crime and six months later, the offenders appeared in court after a series of investigatory activities that included internet protocol (IP) analysis, retrieval of video recordings from cameras installed inside the cybercafe from which the comments had been posted, and the cybercafe’s server data of online activities from certain PCs. The defendants maintained their innocence; however, the court sentenced both to one year of restraint of freedom, which requires notifying the police prior to leaving one’s place of residence, education, or work.\textsuperscript{88}

In March 2013, online journalist and civil society activist Alexander Kharlamov, from the provincial town of Ridder in Northern Kazakhstan, was arrested on charges of allegedly “inciting religious hatred” in his pro-atheism articles.\textsuperscript{89} After spending six months in pre-trial detention, including several weeks in a psychiatric clinic against his will, he was released only to remain under house arrest. He continues to face charges that observers think are caused mostly by his anti-corruption activism, which made him enemies with the local administration.\textsuperscript{90}

On February 5, 2014, the mayor of Almaty hosted a lunch to which he invited several popular bloggers, causing a controversy in the blogging community about whether or not the mayor was attempting to bribe them for more favorable media coverage. Three opposition activists, calling themselves bloggers, attempted to attend the lunch to which they were not invited and staged a protest outside the restaurant when they were refused entry. All three were arrested and given 10-day jail sentences. They were repeatedly detained on the eve of the Almaty mayor’s general meeting with the public, allegedly for libel in the interview following their imprisonment, but since they were freed after only three hours at the police station, their colleagues believed it was more of a “preventive arrest” to block them from disturbing the event.

Dina Baidildayeva, a video-blogger and social media editor at Azattyq.org (a Kazakh subsidiary of Radio Free Europe/Radio Liberty) who frequently engages in protest actions, made a one-person picket to protest the first detention of the trio of bloggers mentioned above on February 8. She was immediately detained but freed with an administrative warning issued by the court.\textsuperscript{91} Several times over the past year, a fake Facebook page alleging Ms. Baidildayeva to be a porn star has been created by unidentified users.

\textsuperscript{87} “New rules of journalists’ accreditation adopted in Kazakhstan,” Internews.kz, August 14, 2013, \url{http://www.internews.kz/newspage/14-08-2013/2878}
\textsuperscript{88} “Клевета в Интернете” [Libel on the internet], January 29, 2013, \url{http://www.nomad.su/?a=13-20130130007}
\textsuperscript{89} Reporters without borders, “Authorities again urged to drop all charges against atheist blogger,” September 5, 2013, \url{http://en.rsf.org/kazakhstan-authorities-again-urged-to-drop-05-09-201345141.html}
\textsuperscript{90} Human Rights Watch, “Kazakhstan: Drop Religious Incitement Charges”, May 22, 2013, \url{http://www.hrw.org/news/2013/05/21/kazakhstan-drop-religious-incitement-charges}
\textsuperscript{91} Joanna Lillis, “Kazakhstan Arrests Four Bloggers in a Week”, February 11, 2014, Eurasianet.org, \url{http://www.eurasianet.org/node/68027}
Since early 2011, anonymizing tools, including proxy sites and specific circumvention software, have increasingly been blocked in Kazakhstan, apparently with no proper court decision issued against them. Users wishing to circumvent censorship use the traffic compression feature in browsers designed by the Opera Software,92 VPNs, and other solutions that are still available. The regulation on public access points bans the use of circumvention tools in cybercafes.93

In March 2012, the Tor Project, whose official website is intermittently inaccessible from Kazakhstan, found evidence that deep packet inspection (DPI) was being used by at least one telecommunications service provider, KazTransCom JSC, to censor and monitor the internet, particularly SSL-based encryption protocols.94 A professional from a private-sector telecom company who spoke on the basis of anonymity stated that the president’s administration, the Office of the Prosecutor General, and the National Security Committee plan to launch three different content monitoring systems, including software to monitor social networking sites (at least one regional administration presumably has such software already). Earlier, in February 2012, a Yvision.kz blogger published a screenshot of a tweet sent by the official account of Kazakhtelecom, which said that their “DPI system provides for traffic management and has no access to users’ personal data.”95

According to Shavkat Sabirov, the president of the Internet Association of Kazakhstan, the DPI system was installed on the backbone infrastructure in 2010 by the Israeli company Check Point Software Technologies.96

In May 2013, a spokesperson for the prosecutor general, Nurdaulet Suindikov, said that the monitoring of media with the purpose to identify extremist and terrorist items was to “be significantly broadened” in 2013–2017, including the monitoring of up to 10,000 websites, mostly foreign ones.97 In October 2013, the prosecutor general’s office admitted that Kazakhstan authorities are “able to selectively block pages” in cases of violations of Kazakhstan laws, including pages on YouTube, but not on Facebook or Twitter. Mr. Suindikov added that several ministries and agencies were working together to “find new technical ways to block sites” and expand the international agreements about fighting destructive content.98 Also in October 2013, a roundtable on strengthening the prevention of terrorism and extremism was held in Almaty, where the deputy head of the city administration’s internal policy unit Aidar Yesenbekov admitted that popular social networking websites like Facebook, Vk.com, and Moi Mir (mail.ru) are monitored.99 On the eve of the protest rally against the abrupt currency devaluation in Almaty on February 15, 2014, several Facebook users, who had stated their intention to take part, reported that police visited their

---

96 As said at the Roundtable “How to make internet safe for children” in Almaty, April 14, 2014.
residences to “discuss their Facebook posts” and warn them against going to an unsanctioned gathering.100

It is difficult to verify reported efforts by the National Security Committee (KNB) or other agencies to monitor internet and mobile phone communications. However, a series of regulations approved in 2004 and updated in 2009 oblige telecom operators (both ISPs and mobile phone providers) 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.101 Providers must store user data for two years and grant access to “operative-investigatory bodies,” including the National Security Committee, secret services, military intelligence, etc., when sanctioned by a prosecutor, or in some cases “by coordination with prosecutor general’s office” or under notification of a prosecutor within 24 hours.102 SIM card registration is required for mobile phone users at the point of purchase under the civil code; however, the requirement is not tightly enforced, and SIM card vendors view the registration as a formality.103

New amendments to the law on countering terrorism signed by the president on January 8, 2013 and effective as of January 18, 2013104 granted extra powers to the security bodies;105 reiterated a vague term of “fomenting social discord,” and obliged all mass media (including online resources and citizen journalists) to “assist” the state bodies involved in counter terrorism. The exact mechanisms of assistance are not specified.

On December 30, 2011, the government issued a decree tightening surveillance in cybercafes. Under the decree, cybercafe owners are obliged to gather the personal information of customers and retain data about their online activities and browsing history. This information is to be retained for no less than six months and can be accessed by “operative-investigatory bodies.”106 Beginning in early 2012, parts of the decree came into force, including the requirement to install video surveillance equipment and filtering software.107 As of early 2014, none of the cybercafes specifically reviewed for this report required an identification card or passport before granting access to internet. The regulation does not apply to public Wi-Fi access points.

---

Since the attack on journalist Lukpan Akhmedyarov in 2012, there have been no reported incidents of physical violence against online users.

The administrators of several independent news sites, such as UralskWeek.kz, Ratel.kz and Nuradam.kz, reported suffering sporadic DDoS attacks apparently as a result of their critical reporting. The origins of the attacks, however, has not been identified and the attacks were not reported to the Computer Emergency Response Team (CERT). Meanwhile, the e-government portal of Kazakhstan became a target for DDoS attacks in December 2013, and CERT undertook measures to localize and block the attacks. The website for government procurement contracts was also attacked and disabled for several hours on March 12, 2014, and in November 2013, the same website was reportedly hacked when unidentified persons published obscene texts there.

Kenya

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td>Free</td>
<td></td>
</tr>
<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>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: 44.2 million
Internet Penetration 2013: 39 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- Two bills—the Kenyan Information and Communications Amendment (KICA) 2013 and Media Bill 2013—were signed into law in December 2013 with provisions that threaten to restrict media freedom both online and offline; the High Court halted implementation of both laws in January 2014 until the full Court considers the legal claims (see Obstacles to Access and Violations of User Rights).

- A new regulatory body, the Communications Authority of Kenya (CA), was created under KICA, though the degree of its independence is debatable due to the political appointment process of its board members (see Obstacles to Access).

- In May 2014, political activist Moses Kuria reported that his Facebook account had been shut down for alleged hate speech (see Limits on Content).

- Additions to SIM card registration regulations were drafted in January 2014 that, if implemented, will provide the communications regulator with unfettered access to mobile network service providers’ subscriber records without a court order (see Violations of User Rights).

- A Vodafone report published in June 2014 included Kenya as one of 29 countries that requested access to user communications data (metadata) on Vodafone networks, while Google’s Transparency Report documented 13 government requests for user account information (see Violations of User Rights).
Introduction

In 2013 and 2014, Kenya’s information and communication technology (ICT) field continued to be vibrant, attracting investments from global ICT giants such as Huawei, ZTE and Cisco, which operate in collaboration with local operators. The country was cited as one of two countries in Africa with the highest internet Gross Domestic Product (iGDPs)—which is the measure of the internet’s contribution to a country’s economy—behind Senegal, even though neither country ranks among the continent’s largest economies, reflecting the respective governments’ concerted efforts to stimulate internet demand.

The growing use of ICTs in Kenya has put a spotlight on issues of freedom of expression and privacy in the country, particularly the problem of hate speech stemming from ethnic tensions that have polarized the country for decades. During the 2007 post-electoral period, hate speech was disseminated via SMS text messages, fueling political conflict and ethnic violence that resulted in the deaths of over 1,200 people. Hate speech was subsequently criminalized with the passage of the National Cohesion and Integration Act of 2008 and the Communications Amendment Act 2009. In the lead up to the country’s general election in March 2013—which saw citizens and politicians alike using ICTs to disseminate information and prevent electoral violence—hate speech shifted from text messages to the internet, particularly on blogs and social media platforms such as Facebook and Twitter. Consequently, the government monitored blogs and social media outlets for hate speech and launched several investigations against bloggers for their alleged hate speech activities. While no major government abuses were reported during the coverage period, the country’s ambiguous efforts to control hate speech online threatened to infringe on freedom of expression and privacy.

There were no known incidents of government filtering or interference with online content over the past year, compared to the previous period when one popular web forum was shut down for failing to moderate hate speech, and text messages were reportedly blocked en masse during the March 2013 elections to prevent political conflict. However, several bloggers faced probes over incitement on social media, and one political activist had his Facebook account shut down for alleged hate speech. Extralegal intimidation or violence against netizens is uncommon in Kenya, though Dickson Bogonko Bosire, the editor of the controversial news blog, Jackal News, was reported missing in September 2013 and was still mysteriously missing as of mid-2014. It is widely believed that his disappearance is not linked to the government.

Two legislative measures passed in December 2013, the Kenyan Information and Communications Amendment Act (KICA) 2013 and Media Act 2013, were seen as posing a threat to press freedom and freedom of expression, both online and offline. While the High Court halted implementation of both bills in January 2014 due to questions regarding their constitutionality, the laws are particularly problematic for their establishment of a Communications and Multimedia Appeals Tribunal under the state-controlled Communication Authority that will have the power to revoke journalists’ press licenses.

---


credentials and impose heavy fines on media outlets and journalists for breach of conduct, among other restrictions.

The September 2013 terrorist attack on the Westgate Mall in Nairobi and the subsequent slew of attacks by the Al Shabab terrorist group across the country has led to a growing sense that the government has expanded its surveillance activities, though the extent of the country’s surveillance capabilities is unclear. In January 2014, the government drafted additions to SIM card registration regulations that will provide the communications regulator with unfettered access to mobile network service providers’ subscriber records without a court order, which if implemented, would contravene constitutional rights to privacy. The proposed regulations also prescribe heavy fines and prison sentences for offending subscribers, agents, and providers. Meanwhile, in mid-2014, Vodafone named Kenya as one of 29 countries that requests access to user communications data on Vodafone networks, and Google’s Transparency Report documented requests for user account information from the Kenyan government for the first time since Google began reporting this data in July 2009.

Obstacles to Access

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 2013, the percentage of the population with access to the internet stood at over 52 percent, increasing from 41 percent recorded in December 2012. By contrast, data from the International Telecommunications Union (ITU) from 2013 estimated a lower penetration rate of 39 percent, up from 32 percent in 2012. Penetration for fixed-line broadband subscriptions remained very low at 0.1 percent in 2013.

Meanwhile, mobile phone subscriptions stood at over 31 million, with a penetration rate of 77 percent (71 percent according to 2013 ITU data, with no notable change from the previous year), 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. As such, internet-enabled mobile phones are the primary drivers of growing internet uptake in Kenya, as citizens turn to their handsets for value-added mobile services such as social media, entertainment, mobile money transfer, and lower cost text messaging applications.

Kenya has comparatively low-priced mobile services for Africa, with monthly costs averaging KES 161.

8 International Telecommunication Union, “Mobile-cellular Telephone Subscriptions, 2000-2013.”
(US$1.90) for 30 calls and 100 SMS text messages. The average user pays about US$36 per month for 1–2 Mbps of unlimited data services and US$37 for unlimited internet through a USB dongle (3G modem). These relatively affordable costs are in large part the result of strong regulatory interventions that have led to the implementation of the lowest mobile termination rates across the continent. 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, and the rise in social media use, particularly among the youth population.

Nonetheless, the cost of mobile devices and internet subscriptions remains a stumbling block for many impoverished Kenyans to access the web, and access to inexpensive quality internet remains far-reaching for many low-income earners, prompting the government to set up a Universal Service Fund in 2013 to raise KES 1 billion yearly from the industry to expand mobile and internet services. According to a Gallup poll published in 2013 on worldwide median income, Kenya has an annual per capita income of US$402. Still, Kenya is ranked by the Alliance for Affordable Internet as the fifth most affordable country in Africa for internet access and 18th in the world, among the 46 total countries examined.

Despite decreasing costs, internet speeds are still slow, averaging 1.9 Mbps (compared to a global average of 3.9 Mbps), according to May 2014 data from Akamai’s “State of the Internet” report. In addition, Kenya’s broadband adoption (characterized by connection speeds greater than 4 Mbps) was about 5 percent (up from 2 percent from the previous year), while the country’s narrowband adoption (connection speed below 256 kbps) is 2 percent (down from 3 percent).

Further, while internet penetration continues to increase across the country, there is still a large disparity in access between rural and urban areas. Internet use in Kenya is mainly concentrated in Nairobi, and significant action is needed to address issues of access outside of the capital. According to a November 2013 report by the McKinsey Global Institute, Kenya’s urban internet penetration rate

13 Mobile termination rates are a measure of the costs that mobile operators charge each other for terminating inter-network calls.
stood at 78 percent (compared to a national rate of 39 percent), with 95 percent of urban Kenyans possessing an internet-enabled mobile phone.²⁰

Kenya has four submarine cables—Seacom, the East Africa Marine Systems (Teams), EASSY, and Lower Indian Ocean Network (LION2)—that have improved available bandwidth, though this has not necessarily made access cheaper as ISPs have yet to pass down reduced costs to retailers.²¹ In addition, large parts of the country, particularly rural areas, 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, roads, and cable security that are often limited in rural areas. Nevertheless, there have been no reports of the government controlling the internet infrastructure to limit connectivity.

To help overcome Kenya's infrastructural challenges to connectivity, Ushahidi—the Kenyan technology non-profit known for its crowd mapping platform created in response to the post-election violence in 2007-08—developed a modem called BRCK in June 2013 that can keep users connected even without electricity.²² Described as a "backup generator for the net," BRCK was designed to work in regions where connectivity is unpredictable and has the potential to vastly expand internet access to remote areas across the continent.²³

Through the country's open market-based licensing process instituted in 2008, competition is present in most segments of the telecommunications market. There are over ten fixed wireless ISPs in Kenya and four mobile phone providers. In 2013, Safaricom dominated the market for mobile phone services with a 68 percent share of all mobile subscriptions.²⁴ The three other mobile operators—Airtel Networks, Essar Telecom, and Telkom Kenya (Orange)—served the other 32 percent of the mobile market. Among the same mobile providers, Safaricom had an even more dominant position in the mobile data and internet sector, commanding 74 percent of the market.²⁵

The competitive setting in the mobile phone and data subsector has notably led to a broad deployment of infrastructure to many parts of the country. There are no restrictions on the number of operators permitted to launch and operate telecommunications infrastructure in Kenya, with both data carriers and cellular licenses allowed to run domestic fiber networks.²⁶ Meanwhile, service providers have formed organizations such as the Kenyan ISP Association, the Telecommunications Service Providers of Kenya, and the Kenya Cybercafe Owners to lobby the government for better regulations, lower costs, and increased efforts to improve computer literacy.

---

Kenya

The Kenya Information and Communication Amendment Act (KICA) 2013, passed in December, replaced the Communications Commission of Kenya (CCK) with the Communications Authority of Kenya (CA) and tasked the new body with regulatory responsibilities over both broadcast and online media. While KICA explicitly enshrined the independence of the new regulatory body, the act was widely criticized for the power it granted to the Cabinet Secretary to appoint the new authority's Board without stakeholder input, in addition to the presidential appointment of the Board's chairperson. Due to these concerns regarding CA's independence—among numerous others regarding KICA in general (see “Violations of User Rights”)—the High Court in Nairobi halted KICA's implementation in a ruling on January 31, 2014. Nevertheless, the government moved forward with replacing the CCK with the new Communications Authority (CA) as the primary regulatory body in June 2014.

Limits on Content

During the coverage period, the government kept a watchful eye over the spread of hate speech on the internet. In May 2014, a political activist reported that his Facebook account had been shut down for alleged hate speech.

There were no reported incidents of internet censorship or content removal during the May 2013 - May 2014 coverage period, and the Kenyan government did not employ any form of technical or administrative censorship to restrict access to political or other content. Kenyans have unrestricted access to social networking platforms and communication applications such as Facebook, Twitter, YouTube, Whatsapp and the blog-hosting site Blogger, all of which rank among the 10 most popular sites in the country.

In the lead-up to the last general elections in March 2013, the government reportedly ramped up its efforts to curb the spread of content that could trigger unrest or incite violence. One website, the popular forum Mashada.com, was shutdown in January 2013 for allegedly failing to moderate hate speech. The website came back online in late April 2013. In another strategy leading up to the elections, the former CCK regulator issued guidelines for mobile phone providers to regulate the

30 In June 2014, the government formally launched the new Communications Authority of Kenya (CAK) website (http://www.ca.go.ke/), shutting down the CCK webpage. Analysts argue the move is in outright contempt of the January 2014 court ruling that halted the KICA implementation. Other analysts contend that the government may argue that there was no specific court injunction on KICA.
transmission of bulk text messages\(^{34}\) and reportedly asked providers to block messages that could potentially incite violence.\(^{35}\) During the elections period, then-permanent secretary of the Ministry of Information and Communication, Dr. Bitange Ndema, announced that mobile phone providers were blocking more than 300,000 text messages each day to prevent electoral violence,\(^{36}\) though no evidence or other reports surfaced to substantiate this claim. Some independent observers believe Ndema may have fabricated or exaggerated the claim to discourage citizens from trying to spread hate speech via text messages.\(^{37}\) Nonetheless, there were no further reports of this practice occurring after March 2013.

Following the 2013 elections, the government kept a watchful eye over the spread of hate speech on the internet. In May 2014, political activist Moses Kuria reported that his Facebook account had been shut down for alleged hate speech.\(^{38}\) Otherwise, Kenya does not actively block or filter internet content, though 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.\(^{39}\) 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.

Intermediaries can be held liable for illegal content, such as hate speech, though they are not required to actively monitor traffic passing through their networks unless they are made aware of illegal content. 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.\(^{40}\) While there have been no reported cases of intermediaries held liable for hate speech to date, the law has encouraged proactive self-regulation by providers in monitoring and moderating hate speech on their networks and platforms. For example, the big media houses in Kenya have developed community guidelines similar to those developed by YouTube as one measure of controlling online

\(^{34}\) According to Article 9.4 of the guidelines, “Political Messages shall not contain inciting, threatening or discriminatory language that may or is intended to expose an individual or group of individuals to violence, hatred, hostility, discrimination or ridicule on the basis of ethnicity, tribe, race, colour, religion, gender, disability or otherwise.” See: Communications Commission of Kenya, “Guidelines for the Prevention of Transmission of Undesirable Bulk Political Content/Messages via Electronic Communications Networks,” September 2012.

\(^{35}\) To do so, service providers reportedly installed a firewall that could detect messages containing particular words, such as “kill,” which were automatically flagged for further scrutiny. See: “Short Message Service (SMS) & The Kenyan General Elections,” Africa Speaks 4 Africa (blog), accessed June 22, 2013, http://www.africaspeaks4africa.org/?p=2550.


\(^{37}\) Based on interviews with independent analysts in Kenya.


\(^{40}\) 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, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/NationalCohesionandIntegrationAct_No12of2008.pdf.
hate speech. According to a spokesperson, Standard Group handles close to 50,000 comments and censors 30,000 on a daily basis. Intermediaries can also be held liable for the transmission of obscene content under the Communications Amendment Act of 2009, which entails a fine of up to KES 200,000, imprisonment of up to two years, or both.

There are no known state-run, government-influenced, or partisan online media outlets. Citizens are able to access a wide range of viewpoints, with the websites of the BBC, CNN, and Kenya’s Standard and Daily Nation newspapers being the most popular news outlets. 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.

There has been a notable increase in the number of blogs in recent years, covering a diverse range of topics from entertainment, fashion, and photography to technology and business. 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 to tackle hate crimes on the internet when needed.

The internet continues to grow as an important platform for political debate and mobilization around critical issues. Additionally, digital media has revolutionized the ways in which netizens and civil society groups in Kenya network, share information, and affect change. For example, in June 2013, Kenyans rallied online using Facebook and Twitter to launch the #OccupyParliamentReloaded campaign in protest against members of parliament (MPs) who were seeking to give themselves a hefty pay raise. The activists succeeded in their efforts, leading the MPs to not only back down from their demands for a pay rise, but also concede to a paycut.

43 Section 84D of the Kenya Communications (Amendment) Act, 2009 states: ‘Any person who publishes or transmits or causes to be published in electronic form, any material which is lascivious or appeals to the prurient interest and its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied therein, shall on conviction be liable to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or both.’
Kenya

Violations of User Rights

Two bills—the Kenyan Information and Communications Amendment (KICA) 2013 and Media Bill 2013—were signed into law in December 2013, with provisions that threaten to restrict media freedom both online and offline; the High Court halted implementation of both laws in January 2014 until the full Court considers the legal claims. The government also increased its efforts to crack down on hate speech spread through social media and blogs. In the aftermath of the September 2013 terrorism attack on the Westgate mall in Nairobi, there was a strong sense that the government stepped up its surveillance efforts. In January 2014, the government drafted additions to SIM card registration regulations that will provide the communications regulator with unfettered access to mobile network service providers’ subscriber records without a court order.

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. Criminal defamation laws remain on the books, waiting to be repealed or amended to conform to Kenya’s 2010 constitution. Meanwhile, existing laws that are inconsistent with the new constitution are considered unconstitutional, and supplementary legislation continues to be developed through the parliament.

The progressive constitution appeared to conflict with two laws passed in December 2013—the Kenyan Information and Communications Amendment 2013 (KICA) and Media Act 2013—which practitioners regarded as a threat to media freedom in Kenya, both online and off. Despite widespread criticism, the president subsequently signed both into laws without revision. In protest against the new laws’ problematic provisions, the Kenya Correspondents Association (KCA), Kenya Editors Guild (KEG), and Kenya Union of Journalists (KUJ) separately moved the High Court in January 2014 to challenge the constitutionality of the two laws, which they argued violated guarantees for the independence of the media regulator. The High Court in Nairobi subsequently halted implementation of both laws until the full court could consider the legal claims. The hearing of the case was scheduled for October 2014.

If implemented in its current form, KICA would establish a government-appointed Communications and Multimedia Appeals Tribunal with the power to hear appeals on complaints initially handled by the Complaints Commission and Media Council of Kenya created under the Media Council Act. The KICA Tribunal would also have the ability to revoke journalists’ press credentials and prescribe minimum educational standards for journalists to qualify. KICA would further allow legislators to revise the Journalists Code of Conduct and impose heavy fines on media outlets and journalists.

---

49 On the grounds that the laws violate Article 34 of the Kenyan Constitution, which bars the state from interfering in the media sector.
53 Fines involve up to 500,000 shillings (£4,160) for individual journalists who breach the journalistic code of conduct and a maximum of 20 million shillings (£167,000) for companies that do so.
for breaching provisions of the code.\textsuperscript{54} The laws explicitly apply to both print and online journalists, though the status of bloggers as online journalists is ambiguous. Some bloggers believe the laws may be used against them given the government’s growing interest in regulating speech on various online platforms.\textsuperscript{55} Another provision in KICA replaces the CCK with the Communications Authority (CA) as the broadcast and online media regulator whose board and chairperson would be appointed by the communications secretary and the president without stakeholder input. Flouting the January 2014 court injunction on KICA, the government launched the new Communications Authority in June.\textsuperscript{56}

Meanwhile, a number of positive laws have been drafted in recent years to protect the rights of Kenyan internet users. The draft 2012 Data Protection Bill, for example, aims to regulate the collection, processing, storing, use, and disclosure of information relating to individuals processed through automated or manual means.\textsuperscript{57} The 2012 Freedom of Information Bill underwent stakeholder consultation in mid-2013 and awaited consideration in parliament as of mid-2014.\textsuperscript{58} Both bills promise to enhance internet freedom in Kenya, illustrating the country’s commitment to the development of its ICT sector and the use of ICTs to enhance public sector accountability.

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.\textsuperscript{59} Individuals found guilty of spreading hate speech, broadly defined, can be fined up to KES 1 million (nearly US$11,000) or sentenced to up to three years in prison, or both. In the past year, the government increased its efforts to crackdown on hate speech spread through social media and blogs.\textsuperscript{60} In May 2014, the National Steering Committee on Media Monitoring recommended that controversial Ugandan scholar David Matsanga be probed for alleged incitement on social media.\textsuperscript{61} It also pushed for the prosecution of seven bloggers who were purported to have used inciting language and extreme hate speech in their social media postings. The committee urged bloggers to cease posting emotive and abusive comments.

The interception of messages and the disclosure of their content is a criminal offence,\textsuperscript{62} though in the lead-up to the March 2013 elections, worries over potential unrest reportedly led the

\begin{itemize}
\end{itemize}
government to implement precautionary surveillance measures to curb the spread of hate speech. A year before the elections in 2012, the CCK announced a requirement for telecom service providers to install an internet traffic monitoring system, which supposedly worked by assigning a unique internet protocol (IP) identity to individual gadgets, effectively making any communication traceable to its device of transmission. In their attempts to reassure consumers that the CCK would not proactively spy on internet users, officials noted that the system “does not have to read and disclose people's information” and “will only monitor traffic.” No further information was revealed about the extent to which service providers complied with the installation requirement or how the system had been put into practice, and no known abuses surfaced during the March 2013 elections or thereafter.

SIM card registration requirements have been in place since 2009 in collaboration with service provider, and were reinforced in January 2013 by the implementation of the Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations 2012, which placed explicit responsibility on mobile providers to record and maintain an index of all subscribers. SIM card registration requirements were more strictly enforced following the Westgate Mall terrorist attack in Nairobi in September 2013. The increased security threat also prompted Kenya to join Rwanda, Uganda, and South Sudan in an agreement to establish a cross-border SIM card registration framework aimed at curbing the rise in crimes perpetrated by mobile devices.

Problematic additions to SIM card registration regulations were proposed in January 2014 that grant the CCK with access to service providers' sites and records without a court order and reportedly prescribe penalties of up to KES 300,000 (approximately US$3,500) for individuals and KES 5 million (US$58,000) for mobile providers, while agents can be fined up to KES 500,000 (US$5,800) or imprisonment of up to one year. Mobile phone providers and consumer rights activists oppose the proposed regulations that will grant sweeping powers to the regulator and contravene constitutional rights to privacy.

There are no known requirements for ICT service providers to proactively monitor their users. However, in the aftermath of the September 2013 terrorism attack on the Westgate mall in Nairobi, there is a strong sense that the government has stepped up its surveillance efforts, though the

67 Section 15. “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.” Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations, 2013, (draft) http://216.154.209.114/links/consultations/current_consultations/Draft_Regulations_on_Registration_2013_Amended.pdf.
extent of those efforts are unclear and unreported. One government initiative proposed in April 2014 aims to register the biometric details of all Kenyans in a new national digital database. In May 2014, the president reportedly asked the Safaricom mobile phone operator to “develop a security communication and surveillance system that would urgently boost the capacity of the national security agencies to fight terrorists.”

In June 2014, Vodafone published its “Law Enforcement Disclosure Report” that included Kenya as one of 29 countries that requested access to user data and communications on Vodafone networks between April 1, 2013 and March 31, 2014. With a 40 percent shareholding in Safaricom in Kenya, Vodafone reported that it was not required to implement the technical requirements necessary for lawful interception and therefore did not receive any demands from the government to assist with the lawful interception of communications. On the issue of user and communications-related data (or “metadata”) requests, Vodafone was unable to report the exact number of requests received in Kenya due to the country’s unclear legal provisions under the Official Secrets Act that prohibit the publication of certain government information. Nevertheless, Vodafone’s report notes that the laws governing the disclosure of communications data in Kenya—such as KICA and the National Intelligence Service (NIS) Act of 2012—all require the authorities to obtain a court order or search warrant for data requests, with the exception of “extreme cases of emergency” during which the Director-General of NIS is allowed to operate without a warrant for up to 36 hours.

Among content hosts and social media platforms, Google’s Transparency Report documented requests for user account information from the Kenyan government for the first time since Google began reporting this data in July 2009. For the reporting period of July to December 2013, 11 account requests were documented with a compliance rate of 63 percent (or 7 requests), while 2 account requests were made during the January to June 2014 period with 0 percent compliance. No requests were reported for user information from Twitter during the coverage period, and Facebook did not have updated data beyond the first half of 2013.

Extralegal violence against online journalists and ordinary internet users is not common in Kenya, though bloggers and social media users often harass each other with inflammatory language and hate speech. In one unusual instance during the coverage period, Dickson Bogonko Bosire, the chief editor of the controversial news blog Jackal News was reported missing in September 2013. Bosire had periodically experienced threats in response to his blog’s coverage of corruption investigations and scandals, and according to Reporters Without Borders, Bosire had gone into

hiding or fled Nairobi on several occasions.\(^76\) As of March 2014, his family still had not heard from him, ruling out an initial theory that Bosire had gone into hiding after he published a controversial blog post about the International Criminal Court (ICC) proceedings against President Uhuru Kenyatta in which he listed the name of an ICC witness.\(^77\) Nevertheless, it is widely believed that his disappearance is not linked to the government.

There were no politically motivated cases of technical violence against civil society or opposition websites during the coverage period. In 2013, the government launched several initiatives aimed at reining in the growing wave of crime perpetrated by use of technology, such as the Kenya Computer Incidence Response (KE-CIRT), the Public Key Infrastructure (PKI), and a National Cybersecurity Master Plan.\(^78\)


Kyrgyzstan

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>35</td>
<td>34</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 5.7 million

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Penetration</td>
<td></td>
<td>23</td>
</tr>
<tr>
<td>Social Media/ICT Apps</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Political/Social</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Bloggers/ICT Users</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Press Freedom 2014</td>
<td>Not Free</td>
<td></td>
</tr>
</tbody>
</table>

Key Developments: May 2013 – May 2014

- There were fewer cases of removal of content during the coverage period compared to the previous period, which saw instances of forced removal of specific online content, such as controversial videos (see Limits on Content).

- In May 2014, the president signed an amendment to the criminal code, which introduced criminal penalties of up to three years in prison for disseminating deliberately false accusations of committing a crime (see Violations of User Rights).

- New legislation was passed in February 2014 requiring the registration of SIM cards (see Violations of User Rights).
Introduction

The environment for internet freedom in Kyrgyzstan has improved over the past few years. Shortly before the overthrow of President Kurmanbek Bakiyev's regime in 2010, political pressure on the media—both traditional and online—intensified. During this time, the video portal Stan.tv was closed as punishment for covering opposition meetings,\(^1\) the country's largest online portal and main platform for political discussion was shut down,\(^2\) and all internet service providers (ISPs) were forced to cut off their connections to the international internet as part of an effort to prevent information from leaking out.\(^3\) After Bakiev's removal in April 2010, however, these restrictions were lifted, and the flow of information returned to normal.

Despite such 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. Over the past few years, the government continued to sporadically block certain types of content that were deemed harmful or indecent, though these incidents have declined 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. Additionally, 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

Access to ICTs has grown in Kyrgyzstan in recent years, with internet penetration rates among the highest in Central Asia, though 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 2013 stood at over 23 percent, an increase from about 16 percent in 2008.\(^4\) In contrast, the SCA reported that in 2013 there were 4 million internet users in Kyrgyzstan, or approximately 70 percent of population.\(^5\)

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


\(^3\) “Блокировка продолжается”[Blocking goes on ], Namba.kg (blog), April 6, 2010 http://blogs.namba.kg/post.php?id=470.


Kyrgyzstan

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 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 internet speed in Kyrgyzstan by the end of 2013 was 2.5 Mbps.

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 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 123 percent as of October 2013, according to the SCA (ITU statistics report a mobile phone penetration rate of 122 percent for 2013). 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. Saima Telecom has launched a 4G network covering Bishkek and some suburbs.

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 there is well-developed infrastructure and 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. 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 costs around US$18 per month. At the same time, KyrgyzTelecom has deployed 34 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 2 GB of data per month at maximum speeds, decreasing to 64 Kbps after reaching the data threshold. This plan costs around

---

US$9 per month. Megacom offers similar options, with monthly 2 GB packages costing around US$10. By comparison, in 2013 the average monthly wage was KGS 11,085 (US$225).  

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. 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.

Many social media outlets such as YouTube, Facebook, and Twitter are freely available. However, some international blog-hosting services are subject to filtering from ISPs based in Kazakhstan. 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 2014. Currently, three out of four of Kyrgyzstan’s first-tier ISPs are linked to the international internet via Kazakhstan and its state-run provider KazakhTelecom; the fourth connects through Russia. As a result, websites that are blocked by the government of Kazakhstan can sometimes become inaccessible to users in Kyrgyzstan as well. For example, sites such as LiveJournal, the news website Newsland.ru, and some Google services have been blocked in Kazakhstan, making them inaccessible for some users in Kyrgyzstan. As of January 2014, only Saima Telecom still receives filtered traffic from Kazakhstan, whereas other ISPs receive unfiltered traffic.

Kyrgyzstan's telecommunications sector is relatively liberalized and competitive compared to that of other countries in the region. The state-owned KyrgyzTelecom is 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. In addition to the first-tier providers, there are 69 licensed second-tier ISPs, though only 15 are active.

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 frequencies for deploying 4G networks, but only 4 of them have begun to use the frequencies for this purpose due to the large investment required in the first stage of deployment. 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. At the same time, the director of SCA stated that Aktel’s liquidation will likely

---

14 Из 12 компаний только 4 подтвердили, что развертывают сети WiMax и LTE в Кыргызстане [Only 4 from 12 companies confirmed that they are rolling out WiMax and LTE networks in Kyrgyzstan] December 5, 2012, http://www.qipi.kg/archives/4092
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.16

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.17 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 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.18 For example, in the run-up to the 2011 presidential elections, the government passed a statute placing stringent regulations on foreign television broadcasts related to the elections and imposing high fines for violations.19 Given the difficulty of parsing content, television carriers chose to cut off access to most foreign television channels—whether they were Russian, American, or European—in order to avoid the fines. By comparison, the websites of broadcasters such as CNN, the BBC, or Russia Today remained available throughout the campaign. Online resources were not affected by this statute as they are not considered to be mass media. There have been several incidents of government entities ordering blocks of online content in the past, though there were fewer cases over the past year.

In June 2011, the parliament passed a resolution instructing the government to block the independent Central Asian news website *Ferghana News*, based on charges that its content could incite national strife.20 In February 2012, the SCA sent letters to all ISPs delineating the requirement

---


19 According to the statute, all overseas channels during an election campaign can only be broadcasted from recorded sources and must not contain any information about candidates that can be considered as propaganda or that can discredit them. See Article 22 of the Constitutional Law № 68, “On elections of the President of Kyrgyz Republic and deputies of Jogorku Kenesh of Kyrgyz Republic,” as of July 2, 2011.

Kyrgyzstan

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 Ferghana 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 Ferghana News was of a voluntary nature and that ISPs were not forced to block the website. 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, KyrgyzTelecom—unblocked the site, though the legal status of the original parliamentary resolution is still unclear.

After Russia passed a law titled “On Protection of Children from Negative and Harmful Information” in July 2012, a group of parliamentarians in Kyrgyzstan initiated similar legislation titled “On protection of children from information threatening to their health and development.” Although almost identical to the Russian law, this act was less specific regarding internet regulation, and critics argued that if it were passed, it could be used as a tool for internet censorship by allowing the government to close down sites without a court decision. The criteria upon which the government would make these decisions were unclear. The proposal sparked public outrage, and an internet movement named Kyrnet.kg conducted advocacy activities that compelled members of parliament to postpone the bill until it could be amended.

In November 2012, the ministry of internal affairs proposed amendments to the law “On Counteraction to Extremist Activities” originally passed in 2005, which would 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. Despite the criticisms, the amendments were passed on May 13, 2013.29 As of May 2014, no list of blocked sites has been created.

According to the legal requirements in place under the 2005 statute “On Counteraction to Extremist Activities,”30 the procedure by which a website can be blocked must first begin with a request to the prosecutor.31 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.

The process by which state authorities block online content has been inconsistent. For example, in September 2012, the video “Innocence of Muslims,” which provoked a wave of protests throughout the world, caused a controversy in Kyrgyzstan as well. On September 19, 2012, the Prosecutor General’s Office filed a claim that asked the court to recognize the video as extremist and ban it from show and dissemination in Kyrgyzstan.32 At the same time, the Prosecutor General’s Office instructed the SCA to take measures to restrict access to the video on YouTube.33 Parliamentarians debated whether the video should be banned and were divided in opinion, with some of them calling to ignore the video and others affirming the need to protest against it. Finally, the parliament issued a resolution to block the video temporarily before the court issued a decision, which violated the constitution and other laws.34 One day later, the court decided to recognize the video as extremist and banned it from show and dissemination in Kyrgyzstan.35 According to a statement at the time by the State Committee of National Security of Kyrgyzstan, possession of the film on any storage device could lead to criminal prosecution.36

The government has also sought to restrict access to terrorism-related content. In 2013 approximately 20 sites were recognized by courts as extremist or as inciting national or religious hatred. According to the decision of the court, these sites must be blocked on the territory of Kyrgyzstan. However, the blocking is not unified: not all sites are blocked and the blocking varies by service provider. According to last amendments to the statute on counteraction to extremist

31 Representatives of the 10th department explained the procedure to the author in a private interview in December 2011.
36 В случае обнаружения фильма «Невинность мусульман» в компьютере или других электронных носителях, их владелец будет привлечен к ответственности – ГКНБ [In case of discovering of the film “Innocence of Muslims” on computer or any electronic devices, the owner will be criminally prosecuted], September 21, 2012, http://www.paruskig-info/2012/09/21/6993
activities, the ministry of justice is required to publish the list of blocked sites, but they have not done so as of May 2014.

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 or 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.

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$200–700.37

Currently there are no specific economic restrictions imposed by the government that negatively impact users’ ability to publish content online or online media outlet’s ability to remain financially sustainable.

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 local 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. Social media applications such as Facebook have not yet gained widespread popularity; however, as of November 2013, there were about 168,000 Facebook users in Kyrgyzstan, three times more than there had been in 2011.38

Several online initiatives were launched in the run-up to the 2011 elections, including the website Politmer.kg, created to allow Kyrgyz citizens to monitor the campaign promises made by the presidential candidates, and the crowd-sourcing website Map.inkg.info, created to document and map election violations. During the pre-election debates, some forum topics were created to collect questions for the candidates.

Perhaps the most successful online mobilization campaign of the past few years came 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 and content providers placed banners over their sites with

38 Число пользователей соцсети Facebook в Кыргызстане достигло почти 170 тыс [Facebook users number in Kyrgyzstan reached almost 170,000], November 29, 2013, http://www.knews.kg/society/40838_chislo_polzovateley_sotsseti_Facebook_v_kyrgyzstane_dostiglo_pochni_170_tyis/
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. 39

Violations of User Rights

The number of prosecutions targeting online journalists and internet users has decreased over the past year in comparison to previous years. At the same time, it appears that the government may be moving toward more restrictions on communications, including passing a law requiring the registration of SIM cards, following the examples of neighboring Russia and Azerbaijan.

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 others), 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. 40 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 reputation. 41 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,\(^{42}\) given that criminal penalties can now be levied for such content and that it is unclear exactly how the law will be interpreted.

In 2013 there were several legal initiatives put forth by members of parliament to pass laws that could potentially have an impact on freedom of expression. One of these was an initiative that was almost identical to a law passed in Russia that obliged NGOs receiving financing from international organizations to register as foreign agents. A draft of the bill was proposed in September 2013 by two deputies, 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.\(^{43}\) This initiative was widely debated and several international organizations expressed concern about its potential effects on freedom of expression and assembly.\(^{44}\) On May 26, 2014, the bill was introduced in parliament, but as of the end of this report’s coverage period it has not been passed.

In the past, journalists and bloggers have been subject to prosecution for posting material online, though there have been no reported cases since May 2013. 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.\(^{45}\) 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.\(^{46}\) 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.\(^{47}\) 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,\(^{48}\) as there were many cases of similarly tactless expressions by other authors in Kyrgyz language media outlets who received no punishment, indicating that the government applies laws selectively.

All traditional media outlets must register with the government. In June 2011, the Prosecutor General’s Office proposed amending the statute that regulates mass media\(^{49}\) to include internet


news websites as a form of mass media, requiring them to have a license and to operate with the same responsibilities as traditional media outlets.\(^\text{50}\) In January 2012, an expert from the Government Office seconded the recommendation;\(^\text{51}\) however, it remains unclear whether online media are to be treated the same under the law as traditional news media outlets.

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 (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.\(^\text{52}\)

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 SORM technology ("system for operational-investigative activities"), and in August 2012, Kyrgyzstan updated its surveillance network to be on the same level as current Russian interception systems.\(^\text{53}\)

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.\(^\text{54}\) In April 2011, the parliament passed a decision to switch off all interception equipment deployed on the premises of mobile phone operators.\(^\text{55}\) However, according to reports from September 2011 by members of parliament, the equipment continues to function.\(^\text{56}\) 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.

---

\(^{50}\) "Генпрокуратура Кыргызстана предлагает «законодательно к СМИ отнести интернет-издания и сайты, зарегистрированные в зоне kg»” [Prosecutor General’s Office suggests "to legalize internet agencies and sites, registered in kg zone, by inclusion them in the list of mass-media"], 24.kg, June 6, 2011, http://www.24.kg/community/101891-genprokuratura-kyrgyzstana-predlagaet.html.


\(^{52}\) Об утверждении Правил оказания услуг подвижной радиотелефонной связи  [On approval of regulations of mobile telecommunication services] 25.02.2014 bit.ly/SszY8W

\(^{53}\) Andrei Soldatov and Irina Borogan, "Russia’s Surveillance State,” World Policy Institute, Fall 2013, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.


\(^{55}\) Resolution of Djogorku Kenesh № 332-V as of 15.04.2011, "On switching off mobile operators’ lawful interception equipment.”

Kyrgyzstan

In 2013, there were several attacks on journalists, though it is unclear whether the attacks were related to the individuals’ reporting. One of the injured stated that he did not exclude the possibility that the attack had been related to his professional activity, though his statement remains unproven. The leader of the Public Association “Journalist” (PAJ) stated that since the political events in April 2010, there have been fewer attacks on journalists and cases of attacks were not related to their professional activities. However, there was at least one documented case over the past year in which a blogger and human rights defender was forced to leave Kyrgyzstan because of harassment. 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.

Amid ongoing ethnic tensions in 2011, there were several reported instances of physical attacks or intimidation of members of minorities associated with news websites. In August 2011, Sokhrukh Saipov, the editor and publisher of the news website UzPress, was brutally attacked, although it is unclear whether Saipov was attacked specifically for his online activities. The website publishes content in three languages about the social and political challenges affecting ethnic Uzbeks in southern Kyrgyzstan. In a separate incident in May 2011, followers of the nationalist Asaba party threatened non-ethnic Kyrgyz staff of the online news agency 24kg.org.

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. 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. In the same month, the news agency Vesti.kg also

58 Хотелось бы, чтобы нападения на журналистов расследовались до конца – Марат Токоев [I would like all attacks on journalists to be investigated completely- Marat Tokoev], November 29, 2013, http://medialaw.kg/?q=node/2412
60 В Киргизии правозащитник Илья Лукаш покинул страну из-за угроз [In Kyrgyzstan human rights defender Ilya Lukash left the country because of harassment], June 14, 2014, http://www.svoboda.org/content/article/25291576.html
63 В этом году в Кыргызстане совершено 10 нападений на журналистов во время выполнения им профессиональных обязанностей [There are 10 physical attacks on journalists happened during performance of their duties in this year] November 9, 2012, http://www.paruskg.info/2012/11/09/71388
65 As reported by the blog at: http://blogs.namba.kg/post.php?id=116481.
reported a DDoS attack on its site, presumably because they had been republishing articles from *Ferghana News*, though the motive remains unconfirmed.

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.

Lebanon

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>Partly Free</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>45</td>
<td>47</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 4.8 million

Internet Penetration 2013: 71 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- Lebanon launched 4G services between March and October 2013 in Beirut, with plans to expand to other regions (see Obstacles to Access).

- For the first time, nontransparent and inconsistent filtering by authorities has led to the blocking of dozens of websites, including nine Israeli websites, a website covering a sexual abuse scandal of a Lebanese priest, and a Beirut city guide (see Limits on Content).

- Online campaigns by women’s rights groups Nasawiyia and Kafa contributed to the passage of a new law on domestic violence (see Limits on Content).

- Aggressive defamation suits by politicians and businesses, coupled with the growing power of the Cybercrime Bureau, resulted in the continuing interrogation of prominent journalists and other users for social media posts (see Violations of User Rights).

- Cyberattacks against political groups, news websites, and social media pages are on the rise, galvanized by an increase in sectarian hate due to the conflict in Syria (see Violations of User Rights).
Introduction

The past year in Lebanon has been defined by protracted political and economic stagnation, paralleled by an upsurge in violence. Lebanon went 10 months without an executive government, finally forming a Council of Ministers on February 15, 2014. The country missed its May 2013 deadline for parliamentary elections and, with the end of Michel Sleiman’s six-year term on May 25, 2014, faced a vacuum in its highest government position—that of the president. Many non-affiliated demonstrators denounced parliament’s decision to extend its term for 18 months, calling it the death of democracy. Hackers took over the parliament's website and called for protests, which went largely ignored.

Simultaneously, repercussions of the Syrian crisis have engulfed Lebanon, as the intensity and frequency of political violence and terrorism—including car bombs targeting civilians and daily battles between militias—have reached levels not seen since the end of the civil war in 1990. The violence has also translated online into heightened sectarian hate speech and increased cyberattacks, coupled with an ironic use of online tools to face the new reality, whether demonstrated in the “I am still alive” app to reassure family and friends after an explosion, or by the Infijarat website, which asks users to predict the place and time of the next explosion.

Lebanese digital activists continue to effectively employ social media for advancing their causes, as well as dealing with the Syrian refugee crisis. For example, a group of activists launched an online campaign to combat the increasing racism against Syrian refugees. The campaign responded online to the decisions of several Lebanese municipalities to impose curfews on Syrian refugees. On the other hand, digital activists continue to face police arrests, interrogations, death threats, and physical assaults. Many unconfirmed reports have claimed attempts by the government and non-state actors to censor or even force the closure of outspoken online forums and social media groups, and activists have voiced concerns about the growing power of the Cyber Crime and Intellectual Property Rights Bureau (Cybercrime Bureau).

Lebanese have historically boasted a strong tradition of freedom of the press and media pluralism, something that was seen as strengthened with the introduction of the internet in 1991 onwards. However, sectarian divisions, bitter partisanship, a vague legal environment, and poor infrastructure—problems that have plagued the traditional media environment for decades—increasingly shape new media and communication technologies. These many issues are often attributed to a struggling economy, constant political turmoil and political corruption stemming from Lebanon’s confessional government system.

4 The Arabic term “infijarat” means explosions.
5 For example, see the Facebook page: “The Campaign in Support of Syrians Facing Racism”: http://on.fb.me/08slwz
7 The internet in Lebanon was first introduced to the American University of Beirut in 1991. Public access started two years later, but the significant diffusion of public internet access did not take off until the mid-1990s when multiple ISPs were established. See http://webscience.blogs.uq.edu.au/1636/history-of-web-in-lebanon/
Lebanon

With this dire backdrop, most of the hope inspired by promises to introduce positive legal, infrastructural, and economic reforms to the Lebanese internet and communications technology (ICT) sector has been dashed. The country that had expected to reconfirm its avant-garde status within the Arab world is now struggling to keep up with its more technologically advanced neighbors. Despite this pessimism, the telecoms sector continues to grow, remaining one of the largest contributors to Lebanon's GDP and some ongoing plans to enhance the sector, such as the recent introduction of 4G services, continue to progress at a slow pace. Nonetheless, these small infrastructural developments have been largely eclipsed by the calamitous political and security realities.

Obstacles to Access

The International Telecommunication Union (ITU) noted that internet penetration has increased from 22.5 percent in 2008 to 70.5 percent in 2013, while fixed (wired) broadband subscriptions per 100 inhabitants has increased slowly in recent years, from 9.71 subscriptions in 2012 to 9.95 subscriptions in 2013. Moreover, the World Bank estimates that Lebanon's mobile internet penetration reaches that of some Arab Gulf countries, which have the highest penetration rates in the region. A Byblos Bank report noted that towards the end of 2013, 3G and 4G subscriptions reached 36 percent of the mobile telecom market. As part of a plan to increase 3G coverage, the Ministry of Telecommunications reported that 400 new antennas were installed in December 2013 and a plan for installing 900 antennas, an additional frequency, and a third channel is in progress. Overall, the number of mobile phone subscriptions has increased over the past five years, from 34.1 percent to 80.5 percent in 2013.

Most consequential was the introduction of 4G mobile services in October 2013, though only to limited areas, with promises from the Ministry of Telecommunications to expand the coverage soon. Still, while 4G access is limited to parts of greater Beirut, 3G connections also remain slow, sporadic, and unavailable in many remote areas, and the security situation has set back many development and maintenance plans. Due to continued clashes in the northern city of Tripoli, 3G transmission stations were hit on multiple occasions between March and November 2013, intermittently terminating 3G services in northern Lebanon. On the eastern border, mobile phone lines in Lebanon have been exposed to infringements from the Syrian mobile network MTN.

---

November 2013, Lebanese citizens living in towns as far as 40 km away from the border reported receiving text messages announcing they have reached Syria and may roam on the MTN network.\(^\text{18}\)

In the past, internet and mobile services were expensive, slow, unreliable, and difficult to access, especially in rural areas and outside of the capital Beirut.\(^\text{19}\) Average internet speeds have doubled since March 2012, but Lebanon’s ranking for internet download speed dropped from 151 to 165, according to Ookla’s Household Download Index.\(^\text{20}\) Lebanon’s upload speed rank is even worse (173th).\(^\text{21}\) Moreover, political disputes between the Telecommunication Ministry and operators have continued to delay network upgrades.\(^\text{22}\) Former Telecommunications Minister Nicolas Sehnaoui said that Lebanese receive only 25 percent of available internet speed and accused the Ministry’s Director-General for Investment and Maintenance, Abdulmenaim Youssef, of withholding the sale of additional international bandwidth to internet distributors.\(^\text{23}\) Youssef has also been blamed for obstructing a project that aimed to extend DSL services to 500 deprived towns.\(^\text{24}\)

Although the government substantially lowered the cost of broadband internet and mobile phone subscriptions in 2011, consumer groups complain that rates remain significantly higher than many other countries.\(^\text{24}\) Lebanon stands in the middle of the regional index regarding fixed internet and mobile broadband prices and is classified as a developing country with lower penetration and higher prices than its regional neighbors.\(^\text{25}\) The total cost of installing broadband internet at home is between US$84 and US$100, while the monthly subscription for DSL ranges from US$13 to US$91.\(^\text{26}\) The monthly subscription fee for 3.9G starts at US$10 for 150MB per month, while 4G starts at US$19 for 750MB per month. Both 3.9G and 4G packages reach US$149 for 40GB per month.\(^\text{27}\) Just two years ago, these prices were 80 percent higher and the high bandwidth packages were not even offered. Nevertheless, these prices remain relatively high considering that in 2012 Lebanon had a gross national income per capita of US$9,705, which translates to US$809 per month.\(^\text{28}\)

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 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

---


\(^{26}\) See for example: Ogero: http://bit.ly/MS0XzC

\(^{27}\) See for example: Touch: http://bit.ly/1dRXxM Higher variants of 3g (enhanced) include later releases such as 3.5g and 3.9g. 3.9g from Touch is the fastest mobile broadband connection in Lebanon with a speed reaching up to 21.6Mbps. Alfa offers 3.5g.

monthly mobile internet pricing equal to the fixed DSL price. More recently, mobile operators introduced eight bundles providing deeply discounted rates for certain disadvantaged customers, reducing some bills by up to 88 percent. The “Bil Khidmeh” bundle provides special rates for members of the Lebanese army, civil defense, and municipality police. The US$10 per month offer includes 60 minutes, 60 SMS messages, and 200 MB of internet. Moreover, 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. Due to enhancements to the telecoms infrastructure, the financial advisory group Business Monitor International expected that information technology (IT) market spending will increase from a growth of 5.1 percent in 2013 to 7.4 percent in 2014, despite the drastic economic impact of the Syrian refugee crisis.

The relatively high prices have not deterred most Lebanese from using internet and mobile services extensively, particularly the youth. Internet usage and digital literacy, however, tend to drop among older and less affluent citizens, as with rural inhabitants. Disruptions to internet services are infrequent in urban areas, but tend to occur more often outside of Beirut. The disruptions are usually caused by technical problems and the inability of the network to handle the increased user load, but last year a mix of political, economic, and natural factors caused many disruptions. To make things worse, Lebanon continues to be liable to frequent electrical blackouts, sometimes lasting several hours per day, especially outside the capital. In May 2013, Lebanon suffered from power outages across all its regions as a result of bad weather, and in December 2013, it underwent additional power cuts due to a lack of government funds to buy oil. Similarly, in November 2013, news reports warned of internet disruptions in case the Telecoms Ministry failed to secure the payment of US$1.6 million to the consortium responsible for the India-Middle East-Western Europe (IMEWE) international cable. The issue was resolved at the last minute; some described it as political.

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). The Lebanese telecommunications industry is government-owned and tightly regulated. Lebanon has two government-owned mobile phone companies, officially named Mobile Interim Company 1 and Mobile Interim Company 2. These operate respectively under the commercial names 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

---

29 Caretaker Telecoms Minister Nicolas Sehnaoui Facebook page, January 20, 2014, [http://on.fb.me/1bEu47U](http://on.fb.me/1bEu47U).
number of subscriptions allowed, there is little competition in the industry and the two companies practically split the market evenly between themselves. The fixed-line telephone and internet network is owned and operated by Ogero, a state company headed by Abdulmenaim Youssef. Ironically, Youssef also occupies a position within the Ministry of Telecommunications that oversees the operations of Ogero.

In addition to running the backbone, Ogero sets internet prices and shares in the management of online subscriptions, together with two dozen private ISPs. Since no law regulates their licensing, private ISPs currently obtain a permit by decree from the Ministry of Telecommunications. In addition, the government has significant control over the processing and approval of user applications for broadband services, which can usually take six to eight weeks. Crucially, political influence can significantly interfere with the allocation of contracts to private ISPs and mobile phone operators.

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 no real authority since the law establishing its powers has not yet been implemented. 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. The Lebanese national committee for transition to digital TV announced it has launched its work plan and its operations to complete the transition from analog to digital by June 17, 2015. Yasser Fneish, senior interconnection expert at TRA, noted that the committee is finalizing the request for proposal (RFP) to purchase the adequate equipment for the digital broadcasting network. However, many of these issues will most likely be held up by political disputes and the more pressing security issues.

42 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.
46 Yasser Fneish, senior interconnection expert at the Telecommunications Regulatory Authority, February 7,2014, Beirut, email interview.
Limits on Content

The past year has witnessed the most aggressive attempts by the Lebanese government to filter ICT content, although such filtering rarely relates to local political issues and is more commonly motivated by economic interests. Social Media Exchange (SMEX) reported that 64 websites were blocked in 2013 and early 2014. The vast majority were gambling or adult escort services. However, the numbers included nine Israeli websites, and a news website that had reported an alleged child sexual abuse case by a Lebanese priest. With some exceptions, most of the websites were only blocked temporarily, and some only by certain ISPs. More importantly, the decisions to block these sites remain unclear and non-transparent. For example, the owners of the city guide beirut.com stated that ISPs Terranet and Sodetel both blocked their site in late December 2013. While they were notified that the telecoms minister requested a court order to block their site, the minister denied the claim. Later, Terranet removed the block but Sodetel kept it in place in January 2014. These non-transparent and inconsistent filtering measures are due to the lack of laws governing internet policy.

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.

While most social media and communication apps are available in Lebanon, certain Voice over Internet Protocol (VoIP) applications are blocked on an inconsistent basis in line with the 2002 Telecom Act. 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. It is important to note that VoIP services are mainly blocked because they cut into government revenues generated by international phone calls. Furthermore, only certain VoIP services are blocked, such as Vonage, while Skype is freely accessible. Blocking some VoIP applications is incurring Lebanon an annual income loss of US$100 million. 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 the selling of VoIP services by private operators if they agree to share revenues with the state. Government officials are arguably hesitant to engage in censorship out of fears that the moves could be seen as unfairly targeting one political-sectarian group. In the past, this has been shown

49 The websites that remain blocked include the news website that reported an alleged child sexual abuse case by a Lebanese priest, all escort and prostitution websites, some poker and betting websites (www.fulltispoker.com, www.pokersstars.net, www.bet365.com/en, www.bettfair.com, and www.williamhill.com), and some Israeli websites: Israeli Ministry of Defense, Israeli Security Authorities, International Management Institute university, Tel Aviv Stock Exchange, and the Israeli Air Force (note that some of these web sites are blocked by the Israeli source). In contrast, these websites were blocked temporarily: A gambling website (www.fring.com) and some Israeli websites (Israel Secret Intelligence service http://mosasad.gov.il, an Israeli website that provides employment resources http://nbn.org.il, and Rabbis for Human Rights http://rhr.org.il).
to quickly galvanize various groups against the government or the state security apparatus, causing unrest.

Although 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. Acting upon a court order, the Directorate for General Security has, in the past, pushed the administrators of Facebook groups to delete comments or close groups that are seen as defamatory. The military intelligence has also interrogated individuals for contacting a Lebanese man living in Israel through Facebook. In addition, intermediaries are legally liable for content posted by users, including domain hosting services and ISPs (for more on libel cases and the arrests of intermediaries, see “Violations of User Rights”).

In a new development this year, Facebook management shut down several Lebanese pages for allegedly publishing Hezbollah-related content, including the Facebook pages “Enta Al-Khabar” (November 24, 2013), “Lebanon Debate” (November 27, 2013), and “Al-Jadeed Online” (November 28, 2013). The latter belongs to a mainstream TV channel.

Despite the evidence of some online filtering, in general, taboo subjects that would normally be banned from mainstream media outlets, such as pornography, content supportive of Israel, and sectarian hate speech, are freely available online. Indeed, the two controversial anti-Islam videos, “The Innocence of Muslims” and “The Innocent Prophet,” remain accessible, despite a September 24, 2012 court decision to ban access to the former in Lebanon. Legal experts have expressed skepticism about the ability of authorities to implement such court orders. A similar example is the Turkish “Fetih 1453” movie, which was deemed insulting to Christianity. It was banned from Lebanese theaters in October 2012 but remains available online. The same goes for a French film featuring a gay couple, which was banned from theaters in October 2013.

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. On July 10, 2013, Hassan Baydoun, administrator of Bint Jbeil (bintjbeil.org), shut down the website for a day after he allegedly received threats from a Hezbollah member. Farah Shaer, director of the short film “Wahabtoka Al Muta’h” (I offered you pleasure), also felt it was not safe to publish his film on YouTube after it was officially banned by the censorship bureau.

Contributing to this censorial culture were the numerous assassinations of journalists and politicians from 2005 to 2011, a period that witnessed significant shifts in power inside Lebanon. This climaxed with the high profile assassination of Prime Minister Rafik Hariri and the subsequent withdrawal of Syrian forces from Lebanon. The more recent assassinations of high profile Hezbollah leaders, ranking Future Movement politicians, and journalists covering the Syria conflict has reminded Lebanese that this dark period is far from over. Nonetheless, even the most controversial topics are openly debated online. For example, although homosexuality remains taboo in Lebanon and laws criminalize “unnatural sexual relationships,” LGBTI rights organizations continue to publish content online despite occasional harassment from security officials. The July 2013 announcement by the Lebanese Psychiatric Society that homosexuality is not a mental disorder was widely circulated online.

Online advertising in Lebanon grew by 29 percent in 2012, but it remains 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. 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 factor 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.

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. 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, 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 the 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.

Civil society groups have used social media widely and effectively to mobilize support for their causes. Women’s right groups, such as Nasawiya and Kafa, have been successful in attracting media attention, mobilizing grassroots support, and achieving changes in discriminatory laws.

---

62 See www.helem.net.
66 Sakr, “Online Advertising Untapped in Lebanon.”
Their online efforts, combined with strategic litigation and advocacy, led to the implementation of tougher sentences for “honor crimes” in 2011,70 and the passing of an albeit diluted law on domestic violence in April 2014.71 Lately, KAFA launched an electronic campaign that aims to collect e-signatures to petition the Lebanese president to refer the domestic violence law back to Parliament.

Furthermore, individual online initiatives have scored victories in crowd-funding for social and humanitarian causes. For example, one day after the library of Father Ibrahim Sarrouj, a Greek orthodox priest who has the second largest book collection in Lebanon, was torched in the northern city of Tripoli, filmmaker Mutaz Salloum started a Facebook event with a group of his friends with the aim of raising $35,000 for rebuilding and restocking the library.72 According to the “Enough Silence: Public Mobilization to Restore Lebanon’s Historical al-Sa’eh Library” campaign, $30,173 was collected as of February 6, 2014.73 Another campaign that brought Lebanese together was “I am NOT a martyr.”74 The online campaign did not succeed in stopping car bombs, but it did spread a strong message against the normalization of explosions and was widely covered by local and international media.75

In addition, civil society organizations have been successful in halting the passage of two problematic online media laws through online campaigning. Activists and businesses delayed and eventually canceled a parliamentary vote on the highly-restrictive “e-transaction law” in June 2010.76 In March 2012, a similar campaign to “Stop LIRA,” the Lebanese Internet Regulation Act proposed by the Ministry of Information, led to a halt in deliberations on the law (for more on the e-transactions law and LIRA, please see “Violations of User Rights” below).

Digital activists were also able to achieve a breakthrough concerning press freedom in Lebanon. On September 17, 2013, in a response to a Facebook call from the journalist Diana Moukalled, several journalists and activists gathered outside a court to support journalist Mohannad Hajj Ali, accused of defamation and inciting sectarian hate (See “Violation of Users Rights”). Due to pressure from activists, his case was successfully transferred to the judiciary, and his lawyer was able to accompany him to subsequent interrogations. Journalists who face similar accusations in the future may be able to use his case as precedent.77

    law-reform-targets-honor-crimes.
    me/1FYSkGA.
74 “I am NOT a martyr” facebook page http://on.fb.me/1qqd811.
75 Mohammed Jamjoom, “Outraged Lebanese protest teenager’s death with #nomartyr campaign “, CNN, January 23, 2014,
    http://cnn.it/LPiYFB; BBC Trending, “#BBCtrending: Lebanon’s #notamartyr selfie protest”, http://bbc.in/1F9qFEG.
    Spotlight/Aug/23/Where-online-activism-meets-offline-action.aspx
77 Meris Lutz, “Journalist scores victory as case transferred from ISF cybercrime unit”, The Daily Star, September 18, 2013,
    http://bit.ly/1FvWgT.
Online mobilization has more recently been used to advance prisoners’ rights. In November 2013, an unidentified prisoner created a Twitter account and a Facebook page for Roumieh prison, highlighting corruption at the prison and exposing the deteriorating conditions from which prisoners suffer. However, not all digital activists have been successful. One of the most publicized failures pertains to the ongoing anti-sectarianism campaign, which took off in 2011 and so far has not achieved any of its goals and has failed to mobilize a critical mass of supporters in the country. Failures in this domain, however, were not related to censorship, but rather to organizational challenges.

**Violations of User Rights**

An absence of laws governing online media, increasing pressure on journalists by the Cybercrime Bureau, and cyberattacks against political or social websites constituted a grave threat to user rights over the past year. Users do not generally undergo a full legal prosecution in the country; rather, prominent figures are summoned and interrogated by the security forces for expressing political views online. This is mainly related to criticism of army officials, although users have also faced interrogations for defaming private companies. 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.

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 provisions in these pre-internet era laws relate 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, the penal code, the Publications Law, the Audiovisual Law, the elections law, and the military code of justice. Three serious attempts to develop new media laws have generated heated national debates in the past three years, although so far, none have generated any concrete results.

Firstly, the e-transactions law, proposed in 2010, required “anyone providing online services” to apply for a license, allowed for “warrantless search and seizure” of information and equipment, and proposed a licensing and regulatory body with broad unchecked powers over e-commerce companies. In early 2012, the Ministry of Interior proposed the Lebanese Internet Regulation Act

---

81 Mapping Digital Media: Lebanon, p. 86.
Lebanon

(LIRA), which applied the archaic 1962 Press and Publications Law to websites and their employees.\(^{84}\) Although LIRA was seen as less problematic than the e-transactions law, it included enough vague language and restrictions to evoke fears of broad censorship.\(^{85}\) For example, LIRA prohibited the publishing of “immoral content,” including matters related to gambling, and did not define which websites were defined as “information websites” and thus were required to register.\(^{86}\) LIRA also prohibited users from managing more than one website at a time and banned anyone convicted of a “heinous misdemeanor or felony” from owning one altogether. As mentioned, both the e-transactions law and LIRA were halted under public pressure.\(^{87}\)

In contrast, the law recently proposed by the Maharat Foundation was drafted through engagement with various ICT stakeholders and attempts to uphold democratic rights.\(^{88}\) Nevertheless, the Maharat proposal has garnered some resistance, mainly from the Lebanese Press Federation, which sees it as a threat to its authority.\(^{89}\) In contrast to the two previously mentioned bills, the Maharat law attempts to regulate print, broadcast, internet, and mobile media, thereby unifying the two main laws that currently regulate the media industry: the 1962 press and publications laws and the 1994 audiovisual law. The Maharat law also abolishes provisions that currently allow for the precautionary detention of journalists “convicted for libelous violations,” removes the distinction between political and non-political media, and no longer requires newspapers to obtain a license.\(^{90}\) The draft law has been stuck in the Lebanese parliament’s telecommunications committee since the government collapsed in early 2013, but even with the new government in place, Maharat activists note that there is no political will at the moment to push this draft law forth. The Arab ICT organization Ġma3 is leading an initiative to study ICT laws in Lebanon and the Arab world and later compare them with ICT laws in the European Union in order to recommend best practices and laws for ICT in Lebanon.\(^{91}\)

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, while defaming the army or other public figures carries a sentence of up to 6 months.\(^{92}\) 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. In the recent past, a handful of cases caught the attention of the media and wider public.


[https://www.eff.org/deeplinks/2012/03/proposed-laws-lebanon-iraq-threaten-online-speech](https://www.eff.org/deeplinks/2012/03/proposed-laws-lebanon-iraq-threaten-online-speech).


\(^{87}\) **Samir Kassir eyes.** (2012, April 11). Activists, Bloggers Stop Lebanese Internet Regulation Act, for Now.  


\(^{89}\) **The Daily Star.** (2013, April 24). Maharat lashes back at Press Federation over draft law.  

\(^{90}\) **The Daily Star.** “Maharat lashes back at Press Federation over draft law”

\(^{91}\) Ġma3, “Ġma3 leading an EU-funded initiative to studying ICT legislation in Lebanon and the Arab world”, January 30, 2014,  

Lebanon

Political leaders and state officials have often abused the slander law to intimidate and silence journalists, especially the archaic laws that forbid insulting the president. This has been bolstered this year by the growing power and activities of the Lebanese Cyber Crime and Intellectual Property Rights Bureau (Cybercrime Bureau) in summoning and interrogating online journalists and bloggers. Online journalists and bloggers are often summoned and interrogated by the Cybercrime Bureau in contravention of the publications law, which “bans security investigations of journalists and requires that such investigations [be] conducted by a judge, in the presence of a lawyer, and away from police stations.” Activists fear this practice increases self-censorship and suppresses freedom of expression online. The Legal Agenda, an NGO focusing on legal issues, highlighted “the danger of assigning separate bodies to investigate online as opposed to offline activities,” which will deny online journalists the legal guarantees afforded to offline journalists. It also called on the government “to limit the Bureau’s powers to technical expertise and knowledge that supports the judiciary” and put a stop to their practices of summoning and interrogating people who publish online.93

On June 18, 2013, the Cybercrime Bureau summoned Jean Assy to answer for insulting the President on Twitter. Assy said he was also interrogated over tweets he wrote in which he was critical of Prime Minister Najib Mikati, former prime minister Saad Hariri, and Interior Minister Marwan Charbel.94 He was released on bail, but in February 2014 the publications court sentenced him to two months in prison.95 A few days later, Assy wrote a public apology to the president.96

On September 11, 2013, the Cybercrime Bureau summoned Rasha al-Amine after she posted on her Facebook page an article calling Samir Geagea a murderer.97 Al-Amine was interrogated for four and a half hours before being released without charges.98 Two weeks earlier, journalist Lokman Slim was interrogated for more than four hours for posting the same article, which had been previously published by Almuhasaba, a news website.99 Journalist Mohanad Hage Ali was also summoned by the Cybercrime Bureau for sharing the article, and was accused of defamation and inciting sectarian strife. His case has been transferred to the judiciary for review.100

On January 21, 2014, Lebanese army intelligence officers interrogated Bilal Hussein, an engineer and activist from Tripoli, because he shared and promoted on his Facebook page a cartoon, published by the Beirut Observer, which criticized army commander Jean Kahwaji. Hussein says he was detained for six hours and kept in harsh conditions. He noted that they tied his hands, blindfolded him, kept him standing, and subjected him to intimidation and insults.101

The Cybercrime Bureau also detains users for libel allegations against private companies. For

97 Geagea is the leader of the Christian right-wing Lebanese Forces political party and a former militia commander.
example, blogger Rita Kamel was interrogated in August 2013 over a January 2013 blog post in which she criticized the Pan Arab Web Awards Academy. She was accused of slander and libel but later released after signing a pledge not to repeat the offense.  

Similarly, the bureau detained blogger Gino Raidy on January 29, 2014 for two and a half hours, without the presence of a lawyer. On June 8, 2013, he had written about cube7, a local subsidiary of an international e-commerce solutions company named Bonofa.  

Raidy was accused of defaming Bonofa and was later released after signing a commitment not to use slanderous terms on his blog.  

This is despite the fact that the bureau stated, on September 17, 2013, that they would no longer detain bloggers, journalists, and activists for interrogation.

On November 25, 2013, Rami Aysha, a freelance reporter for Spiegel Online, was sentenced to six months in prison by a Beirut military court for charges of smuggling firearms. His sentence was later reduced to two weeks. Aysha says he was working on a story about arms trafficking when he was arrested on August 30, 2012 and allegedly tortured while in detention. The precise circumstances behind his arrest remain unclear.

Media reports highlighted numerous cases of extralegal violence and threats against activists and bloggers in late 2013 and early 2014. On May 14, 2013, blogger Habib Battah said he was physically assaulted for taking pictures of historic ruins at a construction site in downtown Beirut. Several men attacked and forced him to erase the photos. When he reported it to a local police station, the officers advised him to forget the issue since he did not have any witnesses.  

On June 28, 2013, while Nasawiya feminist activists were having a farewell party, the bodyguards of member of parliament (MP) Nadim Gemayael demanded them not to take photographs as MP Gemayal was in the vicinity and threatened the activists with their guns.  

On November 26, 2013, several online activists and journalists gathered to protest the arrest of the crew of al-Jadeed channel’s “Taht Ta’ilat el Masooliya” (Subject to Accountability) TV show. Customs security agents ended up physically assaulting the protesters.

In addition, several online journalists and activists received death threats on their social media accounts. For example, on March 20, 2013, activist Rami Olleik received death threats on Facebook warning him not to give an interview to Future TV. Journalist Ramez El-Kadi from Al-Jadeed TV received similar threats on Twitter.

---


In a new and unprecedented development this year, Twitter revealed that the Lebanese government has requested information about the identity of specific online users. Twitter complied with 67 percent of the requests.111 Stories of more extralegal methods used to identify anonymous online users also abound. These cases tend to be low profile and are often underreported out of fears of public embarrassment or due to government intimidation. One well-publicized case from 2000 pertains to Gay Lebanon, a pro-LGBTI rights website. Lebanese vice police tried to force Ziad Mughraby, the owner of the local ISP Destination and son of a human rights lawyer, to reveal the names of the website’s owners. Kamal Batal, director of the human rights organization MIRSAD, subsequently emailed a letter of protest to raise awareness about the issue. Under a military tribunal, both he and Mughraby were convicted of defaming the army and forced to pay a fine of US$219 each.112

Currently, Lebanese law does not place restrictions on online anonymity or encryption software. However, there have been reports that the draft media laws currently being debated behind closed doors in parliament do require some form of registration for news websites, similar to the LIRA proposal. According to an order issued by the public prosecutor’s office on June 7 2013, ISPs are to save all internet log files for a period of one year. The requested data include the username, the user’s IP address, the websites the user is connected to, the user’s location, and the protocols used in the user’s online activity.113 Prepaid mobile phones can be easily purchased around the country without any ID requirements.

The incoming minister of telecom Botrous Harb decided to cancel the mandatory registration of new mobile phones entering the country, a move that was opposed by local mobile phone importers and vendors.114 His predecessor Nicolas Sehnaoui had implemented the IMEI (International Mobile Station Equipment Identity) registration requirement in early 2013 in order to counter mobile phones smuggling. Mobile phone networks use the IMEI to identify stolen or smuggled phones.

The issue of surveillance has garnered much public debate and controversy over the past eight years, which witnessed devastating violence and major political shifts, including a chain of political assassinations (mainly 2005-2008), a 30-day war with Israel (2006), a small-scale civil war (2008), and a political climate that continues to divide the country into two large blocks: the “March 14 Alliance” and the “March 8 Alliance.”115 At issue was the widespread and aggressive surveillance and private data acquisition by the Information Branch of the Lebanese Internal Security Forces (ISF), the United Nations International Independent Investigation Commission (UNIIIC), and the Special Tribunal for Lebanon (STL), which were responsible for investigating the assassinations, particularly that of the Prime Minister Rafik Hariri in 2005 that prompted massive protests and forced Syrian troops out of Lebanon, thereby changing the balance of power. These events created two major political camps: the March 8 Alliance that included Hezbollah and the Free Patriotic Movement, and was viewed as supportive of Syria and Iran, and the March 14 Alliance that included the Future Movement, the Progressive Socialist Party and the Lebanese Forces, and was seen as opposed to Syria and allied with the USA.

115 The past eight years have witnessed major shifts in Lebanese politics, which were triggered by the high-profile assassination of Prime Minister Rafik Hariri in 2005 that prompted massive protests and forced Syrian troops out of Lebanon, thereby changing the balance of power. These events created two major political camps: the March 8 Alliance that included Hezbollah and the Free Patriotic Movement, and was viewed as supportive of Syria and Iran, and the March 14 Alliance that included the Future Movement, the Progressive Socialist Party and the Lebanese Forces, and was seen as opposed to Syria and allied with the USA.
The three organizations enjoyed almost free access to private data between 2005 and 2008, collecting sources as diverse as university transcripts, medical history, and mobile phone records in the name of national security. Their work was largely facilitated by Marwan Hmadeh, the ranking March 14 member and telecommunications minister from 2005 to 2008, himself a survivor of a 2004 assassination attempt.

In general, the laws regulating legal 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 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 communication 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 transactions and other specific data. During their respective periods in office, the ministers argued that large-scale, broad requests from the ISF should be accompanied by a court order.

For example, in December 2012, then-telecommunications minister Nicolas Sehnaoui revealed that the ISF had requested an expansive amount of information on Lebanese citizens for a two-month period of time. In a Facebook post, he called upon “all bloggers, e-journalists, Tweeters and Facebook users and all members of our social media community” to pressure the council of ministers to reject the ISF request. In total, three ministers have had conflicts with the ISF and Prime Minister Najib Mikati, who has struggled to appease both sides and present himself as an independent leader. Most recently, the incoming Cabinet of Ministers approved in its first meeting the handing over to security agencies of telecoms data of all Lebanese, despite strong objections from the March 8 alliance. The politicization of these issues and the failure of any attempts to institute clear regulations remain the most serious problems when it comes to online privacy protection.

In addition, reports of Israeli attempts to infiltrate Lebanon’s telecommunications system abound. Over the past four years, several employees working for mobile and fixed phone operators were arrested for allegedly carrying out clandestine intelligence activities for Israel. There were also

---

116 The UNIIC and later the STL, which were established to investigate the assassination of Lebanese Prime Minister Rafik Hariri in 2005, were later accused of collecting private data not relevant to the investigation, including medical records from a local gynecological clinic that is frequented by the wives of many Hezbollah members.


120 (Acting) Prime Minister Najib Mikati resigned March 2013, partly due to a controversy over the term extension for the ISF chief, which Mikati supported and the March 8 alliance opposed.


Lebanon

numerous reports about spying devices discovered on the network. On November 6, 2013, Lebanese speaker of parliament Nabih Berri said that Israel installed spying equipment along its border with Lebanon. MP Hasan Fadlallah said that there are now 39 listening posts which are able to listen to people’s phone conversations and track people holding their mobile phones. On January 8, 2014, Lebanon filed a complaint to the UN regarding Israeli espionage. Moreover, attempts by the ISF to install and operate surveillance technologies have apparently been halted recently. In fact, a public debate about illegal phone lines, surveillance, and privacy ensued after a May 2011 confrontation between former minister of telecommunications Charbel Nahas and the ISF. The controversy was triggered after members of the ISF blocked the minister and his team from entering a ministry building to dismantle a non-commercial mobile network which was allegedly used by the ISF for intelligence purposes, without government sanctioning or TRA supervision.

When it comes to cybercafes, operators have only a few requirements by which they must abide, including registering their business with the Ministry of Finance for tax purposes and ensuring that all software used in their machines is legal and licensed. Interviewed operators of cybercafes said other matters are left to their own discretion and no special requirements to aid the government exist. Customers are not obliged to register and no monitoring software is installed on machines. They do, however, use firewalls and filters to block pornographic websites, particularly to protect children—a matter that caught media attention in April 2006 and led to the addition of such provisions to the proposed e-transactions law.

In Lebanon, cybersecurity is not governed by legislation. Thus, the country lacks a strategy for immunizing itself against cyberattacks. Cyberattacks are on the rise in Lebanon, especially those emanating from outside of the country. Over the past year, several government and news websites were attacked multiple times. For example, on June 21, 2013, Raise Your Voice (RYV) hacked the website of the Lebanese parliament and posted an event calling for a sit-in outside the parliament to denounce the parliament’s term extension. RYV activists had struck multiple times in 2012 and hacked over a dozen government websites. These attacks—seemingly initiated by a local Lebanese group—often consist of posting comments criticizing the government for its economic and developmental policies, especially in relation to the electricity shortage and the increasing poverty.

The spillover effects of the Syrian conflict also impinged on the Lebanese ICT sphere. In early 2013, groups from Kuwait and Syria hacked the websites of the Lebanese parliament and interior ministry,

respectively, to criticize Lebanese support, or cooperation with, the Syrian government. There were also news reports of cyberattacks against Lebanese banks and financial institutions, with some experts noting the attacks may have been state-sponsored and aimed at disrupting Syrian and Iranian finances.

The online news industry has also been a popular target of such attacks. Most recently, the websites of *Arrouwd* newspaper (April 11, 2013), *Murr TV* (April 16, 2013), *NBN TV* (August 3, 2013), and *Lebanon24* (December 29, 2013) came under attack. *Trella*, a blog about free speech, social justice, and human rights in Lebanon, lost 10 years of content after it was hacked on April 10, 2014. The most significant case remains hijacking of *al-Mustaqbal* newspaper’s home page on April 10, 2013. In a politically motivated attempt to discredit the Special Tribunal for Lebanon (STL), hackers posted the names of alleged witnesses in the Rafik Hariri assassination trial. Some journalists’ personal web sites and social media pages have also suffered from such attacks, such as Paula Yacoubian’s Facebook page (January 18, 2013).

There has been an increase in number of attacks on the websites and the online communication tools of political parties, civil society groups, activists and—most recently—clerics. Such incidents include the attacks on the websites of the Palestinian journalists’ association (June 18, 2013), and the Independence Movement (April 19, 2013). On June 30, 2013, the website of the MP Nadim Gemayel was hacked and a video was posted showing a clash between the MP’s bodyguards and Nasawiya activists. Under the video, a statement read “Lock up your dogs”, in reference to the MP’s bodyguards. On December 29, 2013, the Twitter account of Al-Moustaqbal movement Secretary General Ahmad Hariri was hacked. The hackers posted a sectarian tweet that stated, “No one will be able to defeat Sunnis in Lebanon. We will continue in our path till the end and you will not be able to terrorize us,” along with a picture featuring the late Arab leaders Saddam Hussein, Yasser Arafat,

---


138 Trella.org is a blog by activist Imad Bazzi.


141 For a more exhaustive list, please see: [http://www.skeyesmedia.org](http://www.skeyesmedia.org).


Jamal Abdul Nasser, and Rafik Hariri. On January 24, 2014, “Hizb Shabibet Lobnan Al-Arabi”, a political movement, claimed its site was hacked by a Syrian anti-government group. Most recently, Bkerke, the website of the Maronite patriarchate, was hacked on April 15, 2014. Such cyberattacks are likely to further increase given the controversial topics these political groups champion.

Many of these cyberattacks are dealt with promptly, though the perpetrators are seldom identified and detained. In one reported incident, the Cybercrime Bureau apprehended two Lebanese hackers accused of breaking into emails and Facebook accounts, stealing their owners’ identities, and blackmailing them for ransom. The increase in similar hacking attacks and blackmail attempts has alarmed Lebanese security officials, who remain poorly equipped to deal with them.

---

146 These leaders were all Sunni Muslims, although it is important to note that all of them were secular politicians who led secular governments and political groups, especially Abdul Nasser, Arafat, and Hussein.


Libya

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>19</td>
<td>21</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>45</td>
<td>48</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

- Population: 6.5 million
- Internet Penetration 2013: 17 percent
- Social Media/ICT Apps Blocked: No
- Political/Social Content Blocked: No
- Bloggers/ICT Users Arrested: No
- Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Protestors stormed the headquarters of the Libya Telecom and Technology, making political demands and forcing engineers to cut off internet access to large parts of the country (see Obstacles to Access).

- In February, the General National Congress (GNC) passed a law prohibiting any criticism of the 2011 revolution, as well as insults against GNC members (see Violations of User Rights).

- Online threats and violent attacks on journalists increased. Khadija el-Emame, a reporter with the news website Libya al-Mustaqbal, survived an assassination attempt in Benghazi in August 2013 (see Violations of User Rights).
Introduction

The situation has been tenuous in Libya over the past year, with a political crisis and fighting between different armed militias ongoing. The General National Congress (GNC), elected in July 2012, voted to extend its term in February 2014 and laid out plans for a Constitutional Drafting Assembly to write the new constitution without 60 days.  

The Council of Representatives Law was passed in March, setting the stage for parliamentary elections in June. However, while the creation of Libya’s first democratically-elected government in 60 years was a great step forward, there has not been significant progress toward remedying the country’s legal and institutional challenges. The actions of militias, including armed Islamist groups, offset many of the gains the government has made in removing obstacles to internet access and limits on online content. The overall breakdown in the rule of law, instigated by political turmoil and violence, has also led to greater extralegal attacks on journalists.

The internet became publicly available in Libya in 1998, though prices were excessively high and access was limited to the elite. Thousands of cybercafes sprang up after 2000, eventually offering cheap internet to both urban and rural users. 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. In its initial stages, there were few instances of online censorship in Libya. However, it was not long until the Qadhafi regime 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. Overall, the highly repressive online environment, which included harsh punishments for any criticism of the ruling system, contributed to an extreme degree of self-censorship by internet users.

It has now been three years since the 2011 Libyan revolution, when a popular uprising and ensuing civil war deposed the country’s long-time leader, Muammar Qadhafi, and placed the country on a shaky path to democracy. Overall, the country has witnessed a flurry of self-expression as Libyans seek to make up for lost time under the Qadhafi era, resulting in an increase in news sites, the development of a market for online advertising, and massive growth in Facebook use. However, the civil war also impacted investment in the country’s information and communications technology (ICT) sector, damaging infrastructure and sidelining an earlier US$10 billion development plan for 2020. Laws from the Qadhafi era remain an impediment to freedom of expression. In other cases,
laws that once prohibited criticism of Qadhafi’s revolution have been changed to outlaw criticism of the 2011 revolution or members of the GNC. However, the biggest impediment to free speech remains the threat of extralegal violence by armed militias. Journalists faced assassination attempts over the past year and numerous online threats related to their reporting.

Obstacles to Access

Internet penetration has traditionally been very low in Libya. While the percentage of the population with access to the internet almost doubled from 2008 to 2013, the latest estimates still put penetration at just 16.5 percent. Of these users, an estimated 80 percent use the wireless WiMax service. At present the country has 346 towers in 18 different locations to fulfill the need for WiMax services and internet connections. 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.

Mobile phone use is ubiquitous in comparison. There are over 13 million mobile subscriptions in Libya, representing a penetration rate of 156.3 percent. Prices have dropped systematically since the introduction of a second mobile provider in 2003, resulting in greater affordability. By 2013, the price of a prepaid SIM card from the main provider, Libyana, was LYD 5 (US$ 4). Smartphones and 3G connectivity have been available since 2006, though the prohibitive cost of compatible handsets impedes their wider dissemination.

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 per month (US$ 8), an ADSL subscription was LYD 20 (US$ 16) for a 20 GB data plan, and WiMax 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. Libya Telecom and Technology (LTT) announced a plan to decrease the prices of leased lines up to 45 percent starting from first quarter of 2014 to coincide with the month of Ramadan. The LTT also 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. WiMax modems are in short supply, resulting in high prices for second-hand devices sold on the site Open Souk, Libya’s online marketplace.

---

16  See http://ly.opensooq.com/ or https://www.facebook.com/OpenSooq.Libya it even has a mobile app now.
Many foreign and Libyan organizations and individuals in need of a reliable internet service contract have been driven towards two-way satellite internet technology. As two-way technology has become more popular, connection fees and equipment costs have been lowered. Prices were recently at LYD 800 (US$ 630) for the hardware and a monthly subscription costs LYD 255 (US$ 210) for a fast connection, depending on the number of users.\(^{17}\)

Most people access the internet from their homes and workplaces (particularly those working for foreign organizations or companies), followed by mobile phones, and hotel lobbies. The cybercafe industry, which was decimated in many parts of Libya during the conflict, is starting to return to profitable business through catering mainly to foreign workers and Voice over Internet Protocol (VoIP) calls. The adult literacy rate is last recorded at 90 percent and a wide range of websites and computer software is available in Arabic.\(^{18}\) 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.\(^{19}\) 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 20,000 followers.\(^{20}\) Upgrades have been projected in an effort to respond to demands for increased capacity, such as the laying of the European Indian Gateway and Silphium submarine cables,\(^{21}\) the construction of additional WiMax towers,\(^{22}\) the creation of Wi-Fi hotspots, the installation of a long distance fiber-optic cable within the country,\(^{23}\) and the development of next-generation broadband.\(^{24}\)

According to Akamai, Libya has the world’s slowest internet speeds at 0.5 Mbps.\(^{25}\) ICT experts say this results from poor infrastructure, a lack of quality of service, technology constraints and 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.\(^{26}\)

Libya has seen repeated shutdowns to internet service over the past year due to vandalism and technical disruptions. The internet was cut through much of the country in December 2013 as 150


\(^{20}\) See [https://www.facebook.com/ihateltt](https://www.facebook.com/ihateltt)


\(^{26}\) Interview with ex-Libyana IT engineer on March 2013.
protestors violently stormed the headquarters of LTT, demanding the resignation of Prime Minister Ali Zeidan. Faults caused disruptions in Kufra, Zliten, and other cities at other points in the year. LTT has denied intentionally shutting down service.

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. The tender for the first private mobile network service provider was set to be issued in 2014. 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 have strong ownership ties to the government. The LIPTC owns two mobile phone providers, Almadar and Libyana, while a third provider, Libya Phone, is owned by the LIPTC’s subsidiary, LTT.

The post-conflict regulatory environment remains very unclear. The newly elected government has a Ministry of Communication, but it has expressed no clear vision for the future. Furthermore, disputes over the country’s governance have led to controversy over who is the rightful prime minister of Libya, and consequently the legitimate minister of communication. Many of the policies restricting internet freedom that were promulgated under Qadhafi are still operative. During the Qadhafi era, decisions on licensing were made by the government-controlled GPTC. There was talk in 2006 of creating a new regulator, the General Telecom Authority (GTA), but its status and function remains unclear. Some suspect it was intended to oversee the monitoring of online activities.

Limits on Content

The online media landscape has developed quickly in Libya since restrictions on publishing dissipated with the fall of the old regime. As internet use has increased, so has the market for online advertising, contributing to the overall expansion of Libyan news sites and online services. Facebook in particular has become an important news source for many Libyans. Nonetheless, habits formed during decades of oppressive rule and the continued threat posed by militias both contribute to some degree of self-censorship among users, particularly on sensitive subjects. While these limits on content endured in the past year, it is still too early to tell what direction Libya is moving during this highly fluid, uncertain period.

The defeat of the Qadhafi regime led to a cessation of state blocking in August 2011. Under the various transitional and interim governments, censorship remained sporadic. The transitional
government blocked YouTube to suppress videos documenting human rights abuses by militants, but the platform was available again after the civil war ended in 2011.

Social media services such as YouTube, Facebook, Twitter, and international blog-hosting platforms are now freely accessible. In fact, the “Innocence of Muslims” film that sparked protests outside the American consulate in Benghazi was not blocked by Libyan authorities, although it was made inaccessible by YouTube’s parent company, Google. Facebook was inaccessible for at least one day in 2012, although the LTT attributed it to technical error.31

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.

There is little transparency and no legal framework related to the blocking of websites in Libya, as the regulations have not yet been formulated. Technically, all regulations of the Qadhafi era remain valid. When accessing banned websites, users are shown a message from the authorities to note that the site has been blocked.

The English- and Arabic-language websites of the television channel Russia Today (RT) were accessible in Libya during the coverage period, though they were blocked in 2013. RT had posted an interview with Mahmoud Jibril, head of the National Forces Alliance, in which it was alleged that Libya’s last prime minister under Qadhafi, Baghdadi al-Mahmoudi, was tortured in custody by government authorities after being extradited from Tunisia.32 The Ministry of Communications and Information Technology confirmed that RT was blocked on their Facebook page at the time.33

Prior to the war, “indecency” was prohibited but sexually-explicit sites were never blocked. 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 liberation of Tripoli. The committee was formed of conservative rebel fighters in a bid to be seen as the guardians of public morality. 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.

Though the environment has loosened considerably since Qadhafi, 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 year.34 After the revolution, there was a notable increase in the number of bloggers writing within Libya, particularly writings devoted to political activism, hope for the future, and criticism of the interim government. Nonetheless, many bloggers and individuals choose not to comment

on social taboos such as rape or conflicts between warring tribes and cities. 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 also avoid criticizing the 2011 revolution. It should be noted that many commentators are more afraid of retribution from armed groups and non-state actors rather than the government. Such unseen pressures contribute to an atmosphere of self-censorship and incomplete freedoms.\textsuperscript{35}

After decades of harsh censorship, the online media landscape in Libya is now much more diverse, with few dominant news providers and many local or privately-owned outlets. 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. 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.\textsuperscript{36} The social networking site was the most visited website in the country and has also become the main source of news about Libya for a large number of users inside and outside the country.\textsuperscript{37}

Over the past year, Libyans have used Facebook and Twitter to mobilize around a variety of causes. Recent campaigns include the “No Extension of GNC” movement. 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 and violent protests in Benghazi’s Freedom Square, which quickly spread into violent clashes around the country.

### 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 to outline Libya’s governance during the transitional and interim period following the fall of the Qadhafi regime.\textsuperscript{38} However, the formation of a committee to draft the new constitution was delayed until March 2013, when the GNC established a 60-member constitutional committee.\textsuperscript{39} In the meantime, restrictive laws remain on the books and a murky surveillance apparatus continues to function with little judicial oversight. The gravest threats to user rights, however, come from armed groups. Several online journalists have faced threats and in some cases violent attacks in the country’s highly polarized and tense environment.

During the Qadhafi era, several laws provided for freedom of speech, but these protections were

\begin{itemize}
  \item \textsuperscript{37} “The Top Sites in Libya,” Alexa, accessed May 31, 2014, \url{http://www.alex.com/topsites/countries/LY}.
  \item \textsuperscript{38} “Draft Constitutional Charter for the Transitional Stage,” Libyan Transitional National Council, September 2011, available at \url{http://www.refworld.org/docid/4e80476b2.html}.
\end{itemize}
typically undermined by vague language restricting the same freedoms. For example, the 1969 Libyan Constitutional Declaration and the 1988 Green Charter for Human Rights both guarantee freedom of speech and opinion but also note that these must be “within the limits of public interest and the principles of the Revolution.” A press law proposed in 2007, and a telecommunications law proposed in 2010, were never implemented. Other laws dating from the Qadhafi era provide for harsh punishments 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. 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.”

Since 2012, the judiciary has become increasingly independent. In 2012, the Supreme Court of Libya declared a law that criminalized a variety of political speech unconstitutional, in what was considered a landmark decision as the first time the judiciary had ruled to defend free speech. More recently, however, state bodies remain subject to pressure from a variety of armed militias.

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 that outlawed criticism of Qadhafi’s “Al-Fateh Revolution.”

The breakdown of the rule of law and growing influence of militias has resulted in a worrying uptick in threats and violence against journalists. Khadija el-Emaime, a satellite TV station bureau chief and journalist for the news site al-Mustaqbal, survived an assassination attempt in Benghazi on August 12, 2013. Mahmoud al-Misrati, editor-in-chief of the newspaper Libya al-Jadida, has been repeatedly threatened on social media and was targeted with a rocket-propelled grenade strike against his home in January 2014. George Grant, a British journalist for the online publication Libya Herald, fled Libya in January 2013 following threats apparently sent from Islamist militants. Grant had written an article regarding a suspected “death list” of senior security officials drawn up by

---

Islamist fighters seeking to undermine the state security presence in Benghazi. In early 2014, many more journalists were forced to leave the country due to repeated intimidation.

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. Libyans must present identification when purchasing a SIM card, but extensive efforts were also made to develop the capacity to eavesdrop on Skype and VSAT connections. According to current and former staff of LTT, the government even obtained backdoor access to Thuraya satellite phones, which were widely perceived as a secure means of communication.

While many Libyans would like to believe that such widespread surveillance has ceased, 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 it was 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 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.

Websites are vulnerable to cyberattacks, 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.

---


51 Ibid.


53 Sonne and Coker, “Firms Aided Libyan Spies.”


Malawi

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>11</td>
<td>11</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>42</td>
<td>42</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 16.3 million
Internet Penetration 2013: 5.4 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- In July 2013, the government reinstated a VAT of 16.5 percent on internet services after it was removed only a year earlier (see Obstacles to Access).
- Progovernment commentators on social media platforms seemed to increase, particularly in the lead-up to the tripartite elections in May 2014 (see Limits on Content).
- The draft Electronic Transactions and Management Bill—introduced in October 2013—explicitly provided for freedom for online public communications but included provisions similar to the controversial E-Bill that may threaten internet freedom (see Violations of User Rights).
- In November 2013, an online journalist was arrested for allegedly “intimidating the royal family.” He was held for four days on charges of extortion and eventually acquitted in February 2014 (see Violations of User Rights).
- SIM card registration requirements were announced in January 2014 to be implemented by the end of 2014 (see Violations of User Rights).
Introduction

In 2014, Malawi celebrated the 50th anniversary of its independence from British colonial rule and 20 years of multiparty democracy, which saw the election of Arthur Peter Mutharika to the presidency in May. As the younger brother of and close advisor to the former president Bingu wa Mutharika who died in April 2012, the new president entered his term with a worrisome history of supporting his late brother’s repressive campaign against the media and civil society while in office. Prior to the younger Mutharika’s election, the media environment had improved slightly under Joyce Banda who had assumed the presidency in April 2012, though the Banda government frequently targeted journalists and ordinary citizens for allegedly insulting or undermining the president’s authority. One online journalist, Justice Mponda, was arrested in November 2013 on allegations of “intimidating the royal family” but was acquitted in February 2014 for lack of evidence. Despite President Banda’s hostility towards media criticism, her term oversaw the adoption of a national ICT Policy in September 2013 that established the goal of turning Malawi into a knowledge-based economy and information-rich society. The Banda government also introduced the draft Electronic Transactions and Management Bill in October 2013, which explicitly spelled out freedom for online public communications. The draft bill, however, was also criticized for its potential to limit internet freedom through a provision that would require editors of online public communications services to make their personal information publicly available; another vague provision would allow the government to appoint cyber inspectors to monitor and inspect websites for “unlawful activity.”

Internet freedom in Malawi also remained tenuous during the coverage period due to the government’s seeming intent to increase its mobile phone surveillance capabilities. In June 2013, a parliamentary committee endorsed the installation of monitoring technology called the Consolidated ICT Regulatory Management System (CIRMS)—locally known as the “spy machine”—despite a 2012 court injunction against the system’s implementation. According to some reports, if installed, the machine would allow the regulatory authority 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.

Obstacles to 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

---

5 Chapter 1: Illegal or restricted content, Article 17, Electronic Transactions and Management Bill 2013.
Telecommunication Union (ITU), internet penetration stood at just over 5 percent in 2013, growing slowly from less than 1 percent in 2008.\(^7\) Fixed broadband subscriptions are extremely rare in the country, reaching only 0.02 percent of the population in 2013,\(^8\) while mobile phone penetration in Malawi is also relatively low at 32 percent,\(^9\) compared to an average of 63 percent across the continent.\(^10\)

Very few households have access to the internet at home, thus most users log on at internet cafes, which charge a minimum of MWK 5 per minute, or about US$1.00 per hour, and close at 6pm. However, increasing mobile internet access due to the recent introduction of 3G and 3.75G mobile broadband services has led to declining patronage at local internet cafes. 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 of the country. Nonetheless, broadband speeds are very slow at an average of 1.1 Mbps (compared to a global average of 3.9 Mbps) according to May 2014 data from Akamai's "State of the Internet" report.\(^11\) In addition, Malawi's broadband adoption (characterized by connection speeds greater than 4 Mbps) was 1.5 percent, while the country's narrowband adoption (connection speed below 256 kbps) was about 5 percent among those with access.\(^12\)

Signal coverage on the GSM network for mobile phones reaches 93 percent of the population, making Malawi's GSM coverage one of the highest in Africa.\(^13\) Despite widespread availability, mobile uptake for the vast majority of the population remains low, hindered in large part by high value-added taxes (VAT) on mobile services. According to the mobile research firm GSMA, Malawi levies a 17.5 percent VAT on the purchases of handsets and airtime, the costs of which are borne by consumers.\(^14\)

Taxes also keep the cost of internet access high. In July 2013, the government reinstated a VAT of 16.5 percent on internet services after it was removed only a year earlier. Consequently, many internet cafes increased their rates from MWK 5 per minute to between MWK 15-20 per minute, while mobile providers raised tariffs by 16-25 percent.\(^15\) As of mid-2014, the monthly price of fixed-line internet access cost US$16.50, while a monthly mobile 3G data plan cost about US$24 for 1.5 GB

---

of data. These prices are beyond the reach of the majority of Malawians, whose monthly average per capita income is US$65 (from an average annual income of $780).

A low literacy rate of 64 percent and a significant digital gender divide also hinders progress and access to ICTs in Malawi, while unreliable electricity and the high cost of generator power in the country strain ICT use. Only 7 percent of the country has access to electricity, giving Malawi one of the lowest electrification rates in the world. 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 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.

The high cost of internet access in Malawi is also symptomatic 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.

Another major challenge facing the telecommunications sector in Malawi is the country’s ICT backbone, which 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.

There are 15 licensed ISPs in Malawi, and reasonable competition exists between the providers. 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.\textsuperscript{23} Previously a government-owned entity, MTL was privatized in 2005; at present, Telecom Holdings Limited owns 80 percent of MTL’s shares while the government retains the other 20 percent.

Malawi’s two major players in mobile phone services, Airtel Malawi and Telecom Networks Malawi, together command a mobile teledensity of 18 percent and recently launched 3G mobile services based on UMTS/HSPA technology.\textsuperscript{24} A third mobile operator, G-Mobile, was licensed in 2008 but the rollout of the new network experienced delays. As of 2014, G-Mobile is in court appealing the revocation of its license due to a failure to start services on time.\textsuperscript{25} 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.\textsuperscript{26} Market competition expanded with the introduction of a converged licensing regime in 2010, which has enabled the country’s two fixed-line operators, MTL and Access Communications, to enter the mobile market.\textsuperscript{27}

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 not without political interference as its board is 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.\textsuperscript{28} The director general, 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

During the coverage period, progovernment commentators on social media platforms seemed to increase, particularly in the lead-up to the tripartite elections in May 2014, while the government launched propaganda online news outlets to counter dissenting viewpoints on the internet.

The government of Malawi does not systematically block or filter internet content, and social media platforms are freely available in Malawi, though the government has demonstrated a desire to


\textsuperscript{24} Universal Mobile Telecommunications Service (UMTS) and high-speed packet access (HSPA).


censor internet content in the past. There have been no reports of content removal—even of illegal content such as child pornography or copyright infringement—and service providers are not held liable for content transmitted through their networks.

Online users and commentators practice a degree of self-censorship, though Malawians became less fearful after President Bingu wa Mutharika passed away in April 2012, leaving the presidency in the hands of Vice President Joyce Banda whose tenure oversaw reduced levels of harassment and violence against traditional journalists that were common under Mutharika’s regime. Otherwise, online journalists usually exhibit caution in handling news associated with ethnic, racial, or religious minorities, while online comments have been less cautious and more open to discussing topics of controversial nature.

Progovernment trolls commonly infiltrate conversations on social media and online news websites to attack commentary that is critical of the government. The trolls regularly appear in various Facebook group conversations, suggesting a strategic pattern of infiltration that analysts suspect is government-sponsored. During the coverage period, progovernment commentators on social media platforms seemed to increase, particularly in the lead-up to the tripartite elections in May 2014.

Meanwhile, the government’s news website, MANA Online—launched in August 2012 to compete with dissenting online news outlets in the country—is known as a government mouthpiece. In 2013, the Presidential Press Secretariat established another propaganda online news outlet, Banthu Times, to further help counter dissenting news online. In addition, the UK-based news portal, Nyasa Times, was putatively connected with former President Banda through two journalists who were known to be members of the Presidential Press Secretariat.

The Malawian blogosphere is still in its infancy but is growing, with media publishers such as Blantyre Newspapers Limited hosting bloggers on their websites to enhance their image as independent news sources. Blogging 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. In 2014, the award was presented to Malawian blogger, Gregory Gondwe.

Nevertheless, many Malawian civil society groups have not been able to develop an online presence, primarily because most of the people they serve reside in rural areas where literacy levels are low and access to ICTs is limited or nonexistent. In addition, economic conditions in the country have made it difficult for journalists and media groups to launch online outlets, while the high cost of using the .mw domain—currently being administered by the Malawi Sustainable Development Network Programme (SDNP) 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 businesses having a limited understanding of the internet and their hesitancy to advertise with independent media outlets.

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, voters were able to verify their voter registration on their mobile devices for free, encouraging high voter turnout.  

Violations of User Rights

The draft Electronic Transactions and Management Bill—introduced in October 2013—explicitly provides for freedom for online public communications but includes provisions similar to the controversial E-Bill that may threaten internet freedom. In November 2013, an online journalist was arrested for allegedly “intimidating the royal family.” He was held for four days on charges of extortion and eventually acquitted in February 2014. SIM card registration requirements were announced in January 2014 to be implemented by the end of 2014.

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, which both restrict the media from reporting on the president, among other limitations. Libel is both 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 below).

While existing legislation pertains primarily to traditional media, the Banda administration introduced the draft Electronic Transactions and Management Bill in October 2013 with the goal of providing a regulatory framework for the development of ICTs in Malawi. The draft bill explicitly provides freedom for online public communications but has been criticized for its potential to limit internet freedom. For one, 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. 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, as well as prohibit all types of pornography and penalize offenses with a fine and imprisonment of up to ten years.

---

34 Chapter 1: Illegal or restricted content, Article 17, Electronic Transactions and Management Bill 2013.
35 Chapter 3: Obligations of editors of online contents, Article 24, Electronic Transactions and Management Bill 2013.
36 Chapter 2: Cyber-criminality, Article 43, Section 7(a), Electronic Transactions and Management Bill 2013.
years. The bill concludes with 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. It was unclear whether the government intended the draft bill to replace or supplement the controversial E-Bill that was introduced in October 2012. As of mid-2014, the bill was still under review.

Online journalists are periodically detained and prosecuted for articles posted on news websites. Most recently, Justice Mponda, a correspondent for the online publication Malawi Voice, was arrested in November 2013 for allegedly “intimidating the royal family” in an investigative story about former President Banda’s connection to the theft of millions of Malawian kwacha from government coffers in a scandal known as “Cashgate.” Before his arrest, the ruling party administrative secretary Joseph Chikwemba contacted Mponda to take down the story in exchange for MK 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. Mponda was later acquitted of all charges in February 2014 due to a lack of reliable evidence. He had previously been arrested and charged with criminal libel in October 2012 for allegedly insulting former President Banda and publishing false information. He was subsequently acquitted of all charges in February 2013, also due to a lack of evidence.

Potential restrictions on anonymous communication include SIM card registration requirements announced in January 2014, which are to be implemented by the end of 2014. 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 Mutharika government suspected

---

37 Ten years imprisonment proposed in draft bill, using Zambia’s 15-year 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, Article 45, Electronic Transactions and Management Bill 2013.


39 Malawi Voice was a frequent target of former President Banda, who reportedly criticized the publication for its “misleading and unbalanced” stories.


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 newly elected President Arthur Peter Mutharika.

Government surveillance of ICT activities is suspected in Malawi, in large part due to the regulatory authority's efforts in 2011 to implement technology known as the Consolidated ICT Regulatory Management System (CIRMS), which was locally labeled the "spy machine." Purchased from the U.S.-based company Agilis International for US$6.8 million, the system was ostensibly meant for monitoring the performance of mobile phone companies and improving 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. In October 2011, a court granted an injunction against MACRA's plan to roll out the spy machine, 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 favor of MACRA in September 2014, granting the regulator the right to install the system in accordance with the country's Communications Act.

Under Malawi's new leadership in the post-Mutharika era, there have been no physical assaults, extra-legal detentions, or technical attacks against opposition activists, bloggers, or ordinary users, though harassment and violence against traditional media journalists was prolific under the late president Mutharika.

Malaysia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>15</td>
<td>14</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>44</td>
<td>42</td>
</tr>
</tbody>
</table>

Population: 29.8 million
Internet Penetration 2013: 67 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- News outlets criticizing the government stayed online, despite cyberattacks and disruptions to content in 2013 and 2014, including a BBC blog that appeared blocked on one ISP (see Limits on Content).
- Police accused two bloggers of spreading religious disharmony on Facebook and detained them for eight days (see Violations of User Rights).
- Opposition politician Teresa Kok was charged with sedition for a satirical online video in May 2014 (see Violations of User Rights).
- In 2014, the government said it had denied online news outlets FZ Daily and Malaysiakini print licenses for “sensational” reporting (see Limits on Content).

* 0=most free, 100=least free
Introduction

In the May 2013 general elections, the Barisan Nasional coalition clung to power with just under 50 percent of the popular vote, having lost its two-thirds parliamentary majority in 2008 for the first time since 1969. In the run-up to the 2013 election, officials reiterated commitments not to censor the internet, and prosecuted fewer bloggers. After the opposition mounted its biggest challenge yet on the back of digital mobilization, they demonstrated less tolerance. In May 2014, opposition politician Teresa Kok was charged with sedition for distributing a satirical online video, which also drew physical threats.

Prime Minister Najib Razak publicly promotes internet freedom, and penetration rates are among the highest in the region. Online mobilization was widely perceived as contributing to the opposition’s 2008 electoral gains, but at least eight bloggers were detained in the months that followed, many for sedition or criticism of Malaysia’s royalty, including the sultans who constitutionally rule 9 of the country’s 16 states and federal territories.

“Cyber troopers,” commentators paid by political parties on all sides to attack their opponents, were active prior to the polls, but less so during the coverage period. However, online news outlets covering the opposition faced ongoing cyberattacks and some apparent filtering, though it was not clear if this was executed by the hackers or signaled a more formal intervention by officials or service providers. In January 2014, a BBC blog post about Prime Minister Najib became temporarily inaccessible on at least one ISP, though the government denied blocking it.

In mid-2013, the University of Toronto’s Citizen Lab reported that at least one electronic document containing election-related information in Malay appeared to be spreading spyware to recipients. The government launched an investigation into online news portal *Malaysian Insider* for quoting international reports about that spyware, which could allow authorities to spy on citizens without their knowledge.

Citizens continued to communicate voraciously via social networks in 2014. News websites, once outliers, are now an indispensable part of Malaysia’s information landscape, despite government attempts to deny them access to the print market by refusing to grant licenses. Political gatherings and rallies held since the May 2013 elections saw significantly more coverage online than in the mainstream media, furthering a trend begun in 2011 and 2012. But they have yet to transform the government’s contradictory approach to the internet into a fully free environment.

---

4. The presence of the spyware in Malaysia does not reveal who is employing it, but it is marketed to governments. See, Violations of User Rights.
Obstacles to Access

Internet penetration was measured at 67 percent in 2013. Though one of the higher rates in Asia, this falls short of an ambitious 2012 official pledge to increase it to 80 percent.

A digital divide persists. In 2013, more than 80 percent of internet users lived in urban areas, and penetration remains low in less populated states in East Malaysia, where most residents belong to indigenous groups. 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-2014. Cybercafes also play an important role outside cities.

A 2010 National Broadband Initiative expedited broadband and mobile expansion, partly in cooperation with Telekom Malaysia, the country’s largest—and formerly state-owned— telecommunications company, which retains a monopoly over the fixed-line network. 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. In 2012, the “1Malaysia” affordable broadband package offered decent broadband speeds for under MYR 38 (US$12) per month in five states with lower penetration rates. By 2013, internet centers were expanding to cities, and the government and local councils had introduced schemes to provide free or inexpensive Wi-Fi nationwide. The average monthly cost of fixed internet access is MYR 99 ($30) per month.

Mobile internet access is available, affordable and popular among young people. Mobile penetration surpassed the country’s total population in 2011 and was approaching 150 percent in 2013, indicating that some individuals have multiple phone lines.

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

---

12 Author’s market survey, 2014.
as a means of controlling the traditional media, though this has not been documented among internet companies, perhaps because the 25 private ISPs often have government connections. The two largest ISPs are TMnet, a subsidiary of the now-privatized Telekom Malaysia, and Jaring, which is owned by the Ministry of Finance. The same is true for mobile providers. The largest, 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.

In recent years, some local authorities have introduced restrictions on cybercafes to curb illegal online activities, particularly gambling, which is grounds for 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.

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**

Content manipulation receded after the May 2013 elections, and news websites continued to fend off apparent efforts to block or throttle their content. After the polls, rallies and protests against the result continued to benefit from online organization and news coverage. Many official attempts to restrict content, however, still lack transparency, causing internet users to wonder whether an inaccessible January BBC report about Prime Minister Najib had been censored.

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 June 2013 that he regretted that promise.

While the Malaysian government blocks some websites for violating Malaysian laws, it 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 July 2013, officials said a total 6,640 sites had been blocked since 2008. Many government-linked companies and public universities restrict access to Malaysiakini and other sites perceived as politically sensitive.

Authorities also make administrative requests to content and service providers to restrict information. The MCMC can instruct websites to remove content, including some perceived as critical of the government. Requests are generally nontransparent and lack judicial oversight and avenues for appeal. Issues such as 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, are also considered sensitive. Discussing them can lead to prosecution, so internet users do exercise self-censorship.

Religion is particularly sensitive. In 2009, the MCMC directed Malaysiakini to take down two videos containing sensitive religious and political content. When Malaysiakini’s Editor-in-Chief Steven Gan refused, the MCMC urged the attorney general to prosecute him. As of 2014 the attorney general had yet to pursue the case, although Gan still risks a potential fine of up to MYR 50,000 ($14,300) and up to one year in prison in the first reported case of its kind. In November 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.

Online news outlets represent an increasingly serious challenge to traditional media, with several among the nation’s most popular websites. In October 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 August 2013, but deferred the approval required for a license in early 2014. 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 and 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. Website staff discovered packets of information sent by their servers were not reaching readers, rendering their content temporarily inaccessible on some ISPs. The platforms were all available again within 48 hours. At least two outlets filed a complaint with the MCMC, which never responded.

In January 2014, a BBC blog post describing social media ridicule of remarks by Prime Minister Najib about the falling price of water spinach became temporarily inaccessible on the Telekom Malaysia broadband network under equally unclear circumstances. When asked if a block was in place, Telekom Malaysia referred the BBC to the MCMC, which denied responsibility.

Despite these issues, 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. Social networking is almost ubiquitous. A 2012 article said Malaysians visited social media platforms a staggering 14 billion times a month. Prime Minister Najib leads the way with his own blog and over a million followers on both Facebook and Twitter. 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.

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.

---

33 Polis Diraja’s Facebook page, [http://www.facebook.com/PolisDirajaMalaysia](http://www.facebook.com/PolisDirajaMalaysia).
and denigrate their opponents. 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.

In 2012, the government admitted paying international public relations firm FBC Media MYR 83.8 million ($26.5 million) between 2008 and 2010 to boost Prime Minister Najib’s image abroad. 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. FBC Media, which denied wrongdoing, collapsed in 2011.

Despite these interventions, online tools have been effective for political mobilization and exposing the government’s grip on traditional media. Organizers of recent rallies for political reform, the Coalition for Free and Fair Elections, 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. In 2011, while mainstream media downplayed reports of police brutality against the largely peaceful protesters, internet users circulated nearly 900,000 tweets and 1,600 videos documenting violence, and 200,000 Facebook users petitioned for Najib’s resignation. In 2012, more bloggers and online news portals weighed in to keep people informed about the rally and the security forces’ methods to control it, which included beatings, tear gas and water cannons; print coverage was described as a “near blackout.”

During the coverage period of this report, 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.

Violations of User Rights

Legal harassment remained a primary means for the authorities to intimidate internet users in 2014 with bloggers—and increasingly, social media users—investigated and sometimes charged for online activity. Opposition politician Teresa Kok was charged with sedition for a satirical online video in May. She and online news outlet Malaysiakini also faced threats. Though jail terms are unusual, the threat still prevents many from taking full advantage of Malaysia's dynamic online environment. The May 2013 election also had an impact on user rights, as opposition news websites faced cyberattacks, and a list of candidates circulating online was discovered to contain spyware.

Malaysia's constitution provides citizens with “the right to freedom of speech and expression,” but allows for limitations on this right. While some recent court decisions have disappointed freedom of expression advocates, others show more independence. In December 2013, the government lost its challenge against a court decision granting a print publication license to independent news website Malaysiakini.

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. The government has also pursued prosecutions based on the CMA's broadly worded Section 211, which bans content deemed “indecent, obscene, false, threatening, or offensive,” and Section 233, when such content is shared via the internet. 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.

45 OpenNet Initiative, “Country Profile—Malaysia.”
At the same time, the Security Offenses (Special Measures) Act (SOSMA) replaced the Internal Security Act, which allowed for infinitely renewable detentions without trial and had been used to hold bloggers. The new law provides several improved protections to detainees, requiring police to immediately inform a suspect’s family and reducing the maximum amount of time they can be held without charge or trial. It also includes a provision explicitly stating that “no person shall be arrested and detained...solely for his political belief or political activity.” Despite these improvements, the law also includes restrictive provisions absent in its predecessor. For example, it grants wide-ranging powers for the public prosecutor—and in emergency situations, the police—to intercept communications without the need for a court order in cases involving security offenses.

The government also made changes to the penal code that could allow for punishment of political speech by classifying ill-defined “activity detrimental to parliamentary democracy” as a criminal offence. Civil society groups fear this could render criticism of government officials or policies punishable with jail time, although the law minister said the provision would only apply to violent activities. Meanwhile, the legislative revisions failed to check other problems, including the use of sedition and official secrets charges to harass bloggers and internet users.

No bloggers were serving long-term jail sentences in 2014, though Malaysian authorities have a history of criminally prosecuting online content producers. Police charged at least eight internet users for criticism of the monarchy in 2009, and questioned others. Many prosecutions were dropped, but at least one defendant elected to pay a fine of MYR 10,000 ($2,700) rather than face the threat of trial. Legal proceedings can be lengthy and uncertain, regardless of the outcome.

Police continue to investigate Raja Petra Kamarudin, founder of the blog Malaysia Today, who fled into exile in 2009 to avoid sedition charges and continues to criticize the administration from overseas. In 2012, police charged Syed Abdullah Syed Hussein al-Attas, who blogs pseudonymously as “Uncle Seekers,” with insulting the Sultan in 64 of his posts. Charges against him are still pending.

---

Individuals can file police reports against other internet users. In July 2013, one group said they had asked police to investigate two Facebook users for comments about the king and the prophet Muhammad. Others reported a separate Facebook account in October for posting an image of the prime minister with a woman’s body. In February, a woman was briefly detained for allegedly insulting the sultan of Selangor on her Facebook page. No charges were subsequently reported. In November 2013, Inspector-General of Police Khalid Abu Bakar warned online news portal Free Malaysia Today and its popular columnist Mariam Mokhtar for producing articles he described as “highly seditious,” but no charges were filed during the coverage period.

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 which 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 at the end of the coverage period. Arrests under apparently politicized sedition charges targeting critics and government opponents continued in late 2014. Separately, at least two sedition charges were filed in relation to online content in June 2014.

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. The jail term was deferred pending appeal. In June 2014, after the coverage period of this report, Prime Minister Najib filed a defamation suit against Malaysiakini for two allegedly defamatory articles published in May that compiled readers’ comments.

---

Other criminal cases have involved religion. In July 2013, police detained bloggers Alvin Tan Jye Yee and Vivian Lee May Ling for eight days on charges of sedition and causing religious disharmony after they posted a greeting to Muslims celebrating Ramadan under an image of themselves eating pork on Facebook; they later apologized and removed the post. The couple was separately charged under the Film Censorship Act 2002 with posting explicit images on their joint blog. Each of the three charges they face carries a possible jail term of three to five years; the trial is ongoing. In November, a group filed a police report against another Facebook user for posting an image of pork alongside Islamic symbols under the account name Adlin Abd Jalil. 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.

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. A 2011 government initiative to provide free email accounts to all citizens over the age of 18 prompted fears it would expand the government’s ability to monitor people’s online activities, but was not very popular. SOSMA, which allows for the interception of communications without a judicial order in poorly defined security investigations, also contains scope for abuse.

72 In August 2010, the right-wing group Perkasa lodged a complaint against blogger Helen Ang for authoring an article that questioned the position of Islam in Malaysia; as of 2013, the case was still pending, but observers felt it was unlikely the attorney general would pursue it. “Perkasa Lodges Report Against Blogger,” Malaysian Insider, August 9, 2010, http://www.themalaysianinsider.com/malaysia/article/perkasa-lodges-report-against-blogger/
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 ($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 Malaysians be stored locally, and limits conditions under which the data can be transferred abroad. It was not implemented during the coverage period.

In March 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. 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. In response, the MCMC threatened the site with a fine of up to MYR 50,000 ($15,200) or one year imprisonment for false reporting under the CMA. No charges were filed against the website or its staff. In May, however, Citizen Lab reported they had further identified “a Malaysian election-related document” they characterized as a “booby-trapped candidate list” containing surveillance spyware. 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 February 2014 said a Malaysian government agency was a “current or former user” of Remote Control System spyware marketed by the Milan-based Hacking Team.

Physical violence sporadically affects traditional and online journalists in Malaysia. No incidents were documented during the coverage period of this report, though threats were documented in relation to digital content, including the reward offered to anyone who would hit opposition politician Teresa Kok for the satirical video that prompted her sedition trial. In an unrelated February 2014 incident that nevertheless evoked the protests against Kok—which involved the symbolic use of chicken blood—unknown people splashed red paint outside Malaysiakini offices and left behind a cardboard box containing a dead duck. Malaysiakini lodged a police report over the incident, an apparent attempt to threaten the news portal over its coverage.

---

A graver threat to independent online news outlets and some opposition-related websites is distributed denial-of-service (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. *Malasikini*, was one of many sites reporting on the opposition which was subjected to an apparently coordinated assault before the May 2013 elections. While attacks continued during the coverage period, they did not succeed in disabling any sites.

---

Mexico

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<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>10</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>38</td>
<td>39</td>
</tr>
</tbody>
</table>

Population: 117 million

- Internet Penetration 2013: 43 percent
- Social Media/ICT Apps Blocked: No
- Political/Social Content Blocked: No
- Bloggers/ICT Users Arrested: No
- Press Freedom 2014 Status: Not Free

* 0=most free, 100=least free

**Key Developments: May 2013 – May 2014**

- In November 2013, the Mexican government created a new National Digital Strategy to promote digital government services, wider access to information technologies, and the use of technologies to improve health, education, and security (see Obstacles to Access).

- A constitutional decree issued by the president to reform the telecommunications and broadcasting sectors took effect on June 11, 2013. The decree included new protections on the right to access information, calls for important infrastructural developments, and regulatory measures to promote greater competition in the telecoms market. However, delays over the passage of secondary legislation needed to implement the constitutional reforms characterized much of the coverage period. A new telecommunications bill was finally passed in July 2014, although it contains provisions that could negatively impact privacy rights for internet users (see Obstacles to Access and Violations of User Rights).

- In 2013 and 2014, Mexico continued to be one of the most hostile environments in the world for journalists and bloggers, who are subject to both physical and technical violence, as well as police harassment (see Violations of User Rights).
Introduction

Although Mexico has experienced dramatic growth in internet penetration over the last 25 years, with average connection speeds increasing from 1 Mbps in 2007 to nearly 4 Mbps in 2013, the country still faces challenges in its quest to extend internet access to all citizens. Pronounced disparities separate large segments of the population from access to information and communication technologies (ICTs). Online publications have faced severe cyberattacks, journalists have received death threats, and some have even been murdered. Despite a recent law aimed at breaking up Mexico’s telecommunications monopoly, to date, six private companies dominate the industry, offering broadband service at prices beyond the reach of many low-income families. And while widespread civil society action resulted in the 2013 passage of a constitutional amendment guaranteeing access to the internet as a civil right, its implementation has been hampered by a lack of supporting secondary laws.

Regional disparities also create a stark digital divide, in which those living in large cities have much greater access to affordable internet service than do those in smaller towns and more remote areas. This issue is particularly pronounced in rural areas due to infrastructural deficiencies and high prices—challenges that are exacerbated by the concentrated ownership of the telecommunications sector by a handful of influential companies.

Although the June 2013 constitutional reform on telecommunications included positive provisions intended to combat monopolization in the industry and guarantee internet access as a fundamental right, there was a delay in the implementation of the secondary legislation required to enact the decree, which was supposed to be passed by December 2013. Congress finally approved the required secondary legislation in July 2014 (outside of this report’s coverage period); however, the legislation contained a number of provisions that threaten the privacy of internet users.

In recent years, physical and electronic attacks have rendered online journalists and bloggers susceptible to the same level of danger faced by traditional journalists. The June 2012 Law to Protect Human Rights Defenders and Journalists establishes a government mechanism of protection and allows federal authorities to investigate attacks against journalists and human rights defenders. Although this is a positive step, to date, the real world impact of the legislation has been minimal. In April 2014, the protection mechanism came under criticism due to delays in processing approximately 60 percent of the 152 time-sensitive requests for protection. Nonetheless, there is at least one documented case of the law being used successfully to assist a threatened online journalist (see “Violations of User Rights”).

---

Obstacles to Access

Internet penetration in Mexico has increased significantly in recent years, growing from 22 percent in 2008 to 44 percent in 2013. Although some optimistic experts expect internet penetration to increase even further by the end of 2014, a pronounced digital gap still exists. Internet penetration in Northern states (including the Federal District) was measured at 44 percent in 2013, yet official sources counted internet penetration in Southern states (such as Chiapas, Oaxaca, Guerrero, and Michoacan) at only 16 percent.

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), 31 percent of Mexicans had household internet access as of 2013, but most did not connect via broadband. Although the number of Mexicans with broadband access has increased over the past decade, growing from 0.42 percent in 2003 to nearly 12 percent in 2013, Mexico still falls significantly below the broadband penetration rates of other OECD countries, which have an average rate of approximately 27 percent. As compared to a minimum wage of US$150 per month, the high price of broadband service in Mexico, which ranges from US$26 to US$73 per month, is a significant factor in the country’s low broadband penetration rates. With an average monthly fee of US$68, cable broadband services in Mexico exceed the average global price of US$60.

Although 84 percent of all internet users in Mexico access the internet from home, in 2013, a large number of users sought access from other locations. Of those who accessed the internet outside their homes, 40 percent utilized internet cafes, 28 percent connected from school, and an additional 28 percent accessed the internet from the workplace. Although the number of cybercafe users is still fairly high, it has begun to decline in recent years, due to increasing personal subscriptions as well as the expansion of alternate public access points. Such diversification has created greater opportunity for Mexicans to access the internet and is, accordingly, helping to reduce regional and socioeconomic internet gaps.

The emergence of mobile technologies has also helped to increase internet access in Mexico. According to an independent study, 64 percent of all Mexican internet users connected to the web...
through mobile devices in 2013. This figure represents an increase of nearly 100 percent in comparison to 2012, when only 34 percent were estimated to use mobile devices for internet access.\(^9\) Notably, mobile broadband penetration, which grew to nearly 14 percent as of mid-2013, has now surpassed fixed-broadband household penetration, which reached 12 percent in the same timeframe.\(^11\) Mobile broadband appears poised to continue growing at a far faster rate than fixed-broadband in Mexico, increasing by 34 percent in the second quarter of 2013, while fixed broadband connections increased by only 8 percent in the same period.\(^12\)

While six private companies primarily control Mexico’s mobile phone sector, Carlos Slim’s America Movil, which counts both Telmex and Telcel as subsidiaries, dominates the information and communication technology (ICT) landscape with 80 percent of landline subscriptions and 70 percent of the wireless market.\(^13\) Top competitors Axtel and Movistar account for only 6 percent of fixed lines and 20 percent of wireless connections, respectively.\(^14\) Mobile phone access is significantly more widespread in Mexico than is internet use, with about 100 million subscribers (approximately 86 percent of the population) as of late 2013.\(^15\)

Such accelerated growth is due in part to a recent drop in prices for mobile phone use,\(^16\) the increasing availability of smartphones, and promotions that narrow the price gap between basic phones and smartphones.\(^17\) As of December 2013, 27 million of the country’s 100 million mobile phones were smartphones.\(^18\) Mexico is reportedly home to the largest smartphone market in Latin America,

---

16 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: Revista Opcion “Cofetel Reduces Interconnection Fees” [in Spanish], Revista Opcion, June 10, 2011, http://www.revistaopcion.com/tag/de-mayo/.
followed by Brazil, Chile, Peru, and Argentina. Further, Mexico’s smartphone market is expected to grow 40 percent as of the end of 2014. In mid-2013, the parliament passed a bill to amend the constitution in order to make a series of reforms to the telecommunications and broadcasting sectors. A Constitutional Reform Decree was subsequently enacted by the Mexican president on June 10, 2013, taking effect one day later.

From a rights perspective, the decree made access to connectivity a fundamental right under Article 6 of the constitution, thereby responding positively to a civil society campaign on the issue. This includes “the right to access information, broadcasting and telecommunications services, including broadband and the Internet.” The reform also defined telecommunications as a public service, thereby making the government responsible for such things as guaranteeing universal coverage, quality, and competition.

On the regulatory side, the decree established two new, independent regulators—the Federal Telecommunications Institute (IFETEL or IFT) and the Federal Commission for Economic Competition (FCEC). The IFT was tasked with implementing a “180 Day Agenda” within 180 days of its launch date, and will have the power to unilaterally punish noncompetitive practices with the withdrawal of corporations’ licenses, the application of asymmetric regulation, and the unbundling of media services—stipulations that could significantly change the Mexican ICT landscape. Restrictions on foreign direct investment and ownership in telecoms were also lifted. Prior to these changes, a 2012 report from the Organization for Economic Cooperation and Development estimated that costs related to the lack of competition in Mexico’s telecoms sector were US$25 billion per year.

From an infrastructural development view, the decree also calls for the establishment of a National Policy for Universal Digital Inclusion and a National Digital Agenda, and places constitutional requirements to expand the national fiber-optic backbone and create a wholesale wireless network.

The decree called for the passage of two pieces of secondary legislation in order to implement the constitutional reforms. A new Federal Economic Competition Act passed both houses and was made law on May 23, 2014. A December 2013 deadline to pass a new Telecommunications and Broad-

---

casting Act, however, was not met. Instead, the bill was introduced to the senate in March 2014 and passed both houses of congress in July 2014, coming into effect one month later. However, this legislation included requirements on providers to store user data and provide law enforcement with real-time location data for mobile phones, as well as allowing providers to block access to certain content—provisions which could significantly infringe on internet users’ rights and which were met with vocal opposition (see “Violations of User Rights”).

In November 2013, the Mexican government created a new National Digital Strategy to promote wider access to information technologies, digital government and transparency, and the use of technologies to improve health, education, and security. A new office manned by presidential staff will coordinate the Strategy, which is not a separate body predicated on internet governance, but is instead an office establishing presidential advisors on digital and internet related issues. Representatives of this office attended the October 2013 Internet Governance Forum, an international multi-stakeholder conference that took place in Indonesia. Along with 20 other nations, the Mexican government endorsed a declaration of the Freedom Online Coalition to advance internet freedom via coordinated efforts of civil society and private sector representatives to support human rights and freedom of expression online.

Although the government of Enrique Peña Nieto has been active in defining a digital strategy and policy, further steps are missing from the government’s internet initiatives, such as the approval of positive secondary legislation that would make universal access to the internet in Mexico a reality.

**Limits on Content**

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. Despite ongoing threats to their security, activists make regular use of social media to provide critical warnings to local communities about dangerous cartel-related situations. Civil society groups have also made use of the internet to generate awareness and activism for causes related to internet freedom, human rights, and other issues. 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 for writing about issues of local corruption and crime.

---


Applications such as Facebook, Twitter, YouTube, and international blog-hosting services are freely available in Mexico and have enjoyed steady growth in recent years. Mexico has the second largest community of Facebook users in Latin America after Brazil—and the fifth largest in the world—with an estimated 38 million users. The number of Mexicans with Twitter accounts has also ballooned in recent years, growing from 146,000 in February 2010 to more than 12 million in early 2014. The president and members of his administration also hold Twitter accounts, using them primarily for disseminating political information.

In early 2013, news broke of an agreement between the Federal Security Council and some state governments to refrain from reporting on violence unless absolutely necessary. This decision was the product of a dual campaign to ease fears about security within Mexico and to present a more positive image to the international community. Such a policy underscores the importance of online journalists’ efforts to report on the full scope of events in their communities, providing critical warnings to neighbors on issues of safety and security that would otherwise be kept quiet by local government officials.

Self-censorship has also been increasing among online journalists and bloggers in the wake of the 2012 murders of several social network contributors who had been posting information about cartel-related violence. Despite such grave threats, however, many brave bloggers and social media users have continued their quest to provide security warnings, address corruption scandals, and otherwise attempt to improve life in their communities.

Economic constraints also influence the diversity of media in Mexico. Scarce funding and lack of interest in online advertising create challenges for individuals and nonprofits seeking to establish sustainable online outlets. 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. Despite such challenges, however, efforts to develop politically oriented websites that are financially independent have continued in recent years.

Among the most striking examples of successful independent digital media is Animal Político, a popular site that counts more followers on Facebook than any other news outlet in Mexico. In order

---

to raise revenue for the site without compromising content based on advertisers’ political leanings, Animal Político is now engaging in brand journalism, offering social media consulting and digital content to private companies. Additional financing is derived from syndicated content and private sponsorships. Animal Político’s approach appears to be unique among Mexican media, and the site has been receiving millions of visits every month since July 2012.

Even outlets that do not depend on government funding have been subject to manipulation from local officials attempting to suppress critical information and to turn the tide in their favor. A handful of bloggers have argued that links on Twitter intended to take users to security warnings were redirecting traffic to a website supported by advertising from the Veracruz government. The governments of Veracruz and Quintana Roo have also been accused of creating groups of social media users who saturate Twitter with publicity favorable to them, and who launch cyberattacks against critical journalists and bloggers.

In January 9, 2014 Noticaribe, an online news portal in Quintana Roo, claimed that its Twitter account had been hacked and used to distribute information favorable to the local government. Although Noticaribe managed to recover control of its Twitter account, other publications frequently running stories about local corruption suffered cyberattacks in a widespread campaign of disinformation. Luces del Siglo, a weekly magazine based in Quintana Roo, argued that the local government cloned the magazine in early December 2013 and then distributed a version missing information about alleged cases of corruption. Although a public relations officer said that the local government respected freedom of expression and had nothing to do with the incident, a fake Twitter account bearing the name of the magazine, @LucesdelSiglo, is still actively impersonating the publication, and is allegedly supported by the state governor. The organization ARTICLE 19 also reported two additional cyberattacks against news outlets in Zocalo and El Noroeste in July 2013.

Attempts to censor content on the websites of regional newspapers occur in other parts of the country as well. The editor of a local newspaper in Nuevo Laredo, Tamaulipas, said the online edition has suffered a series of cyberattacks suppressing comments from citizens in stories concerning corruption of local authorities.

---

37 “La Guerra Sucia,” [Dirty War], Twitter page of @Javier_Duarte, http://chuynews.blogspot.com/2013/05/la-guerra-suica-de-javierduarte-en.html
39 On January 9, 2014, @Noticaribe posted the following information about irregularities on Twitter: “AVISO: Usan en mensajes por cel y redes nombre de Noticaribe para exculpar a funcionario de supuestas irregularidades pic.twitter.com/GpVYyppJH” https://twitter.com/Noticaribe/status/421329777237049344
41 For more, see the following status updates of the Twitter page of Luces del Siglo: https://twitter.com/Lucesdelsiglo/status/411694401954390017 and https://twitter.com/Lucesdelsiglo/status/41159828372366432
Facebook, Twitter, and YouTube are widely used in Mexico, and are playing an increasingly important role in the gathering and dissemination of information about risks in high intensity drug trafficking areas and in mobilization on social and political issues. Citizens reporting on such issues use Twitter hashtags such as #VeracruzFollow to exchange information about acts of violence in their cities. Those contributing to the effort to improve citizen safety have been hampered by a flood of unrelated updates generated by a digital “army” utilizing the hashtags for trivial gossip. Although the leader of the army is unknown, some believe that the operation to distract citizens from useful updates is supported by local politicians trying to suppress news of violence in their communities.

Digital tools have also aided mobilization on social and political issues. 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 include internet access as a fundamental right. Due in large part to the success of the coalition, Congress included internet access as a civil right in its 2013 reform of the Mexican Constitution.44

Violations of User Rights

Violations of user rights have continued to escalate in Mexico in recent years. In 2014, Reporters Without Borders listed Mexico among the most dangerous countries in the world for media personnel.45 Threats and violence from drug cartels—and occasionally from members of local government—have continued to plague online reporters, resulting in at least one murder since May 2013. Cyberattacks have also continued, at times disrupting service to online media outlets. In recent years, legislation has been passed that both positively and negatively impacts user rights. While a law intended to safeguard journalists and human rights defenders is a step in the right direction, a new surveillance protocol jeopardizes user rights by allowing significant breaches of privacy.

The Mexican constitution guarantees freedom of speech, freedom of the press, and privacy of personal communications; however, recent reports concerning a ubiquitous state surveillance apparatus and a new geolocalization law call such protections into question. There are no legal ramifications for online activity other than defamation or libel, although criminal defamation statutes still exist in 13 of Mexico’s 32 states.46 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 event harassment of online journalists.

In June 2012, the Law for the Protection of Human Rights Defenders and Journalists was passed in Mexico, effectively establishing mechanisms for the protection of media workers and NGOs.47 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 April 2013,

---

27 of Mexico’s 32 states had signed agreements to this effect.\(^{48}\) 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 actualize the law has been lacking. A separate amendment, predicated on protecting freedom of expression, was passed in the senate in April 2013. If signed by the president, the amendment will grant authority for prosecution of crimes against journalists to the federal government, marking another positive step in the fight to protect reporters and bloggers.\(^{49}\)

Government agencies in Mexico have also been issuing more requests for content removal and user data in recent years. Between January and June 2013, Facebook received 78 requests from the Mexican government for information related to 127 users. In 38 percent of the cases, Facebook released some information.\(^{50}\) In the same period, Google received 11 requests from Mexican authorities for the removal of content; the company complied with 18 percent of the requests.\(^{51}\) Google also received 83 requests from the Mexican government for user data, producing information in 39 of such cases.\(^{52}\)

Apart from a 2008 requirement that cell phone users register with the government (revoked in 2012) there are no official restrictions on anonymous communication. Despite a constitutional requirement that any interception of personal communications be accompanied by a judicial warrant,\(^{53}\) reports published in 2012 allege that secret surveillance of private citizens is widespread in Mexico.\(^{54}\)

In July 2012, evidence was leaked (and later confirmed by the Mexican army)\(^{55}\) pertaining to the secret purchase of approximately MXN 4.6 billion (US$355 million) worth of “spyware” engineered to intercept online and mobile phone communications.\(^{56}\) In addition to recording conversations and gathering text messages, email, internet navigation history, and contact lists, the surveillance software is also capable of activating the microphone on a user’s cell phone in order to eavesdrop on the surrounding environment.\(^{57}\)

The website of the Mexican Access to Information agency (IFAI) makes no mention of this expen-

---


\(^{50}\) Facebook, “Government Requests Report, Mexico, January-June 2013,” \[https://www.facebook.com/about/government-requests\].


\(^{56}\) Robert Beckhusen, “U.S. Looks to Re-Up its Mexican Surveillance System,” Wired online, May 1, 2013, \[http://www.wired.com/dangerroom/2013/05/mexico-surveillance-system/\].

diture or of the U.S. State Department's alleged assistance in the tripling of Mexico's surveillance capacity via the 2006 installment of specialized surveillance equipment.\(^5^8\) Mexico's "Technical Surveillance System" allows the government to "intercept, analyze and use intercepted information from all types of communication systems operating in Mexico."\(^5^9\) In the past year, reports have 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.\(^6^0\)

Mobile internet users in Mexico will also be affected by a recent law that allows police to locate mobile phones in real time without a court order.\(^6^1\) The bill, which allows the government "warrantless access to real time user location data,"\(^6^2\) became law in January 2014, despite opposition by human rights organizations.\(^6^3\) Although the law is intended to combat drug cartel activity, its lack of independent oversight leaves it open to misuse by police, military, or intelligence agencies. Critics of the law warn that it is unconstitutional and sets a worrisome precedent of warrantless surveillance.\(^6^4\)

Corruption and weak rule of law among state governments—including the infiltration of law enforcement agencies by organized crime—also leave room for abuse should private communications fall into the wrong hands.

Heightening the threat posed by real-time warrantless surveillance, over the past year, online journalists and social media users have reported frequent harassment, occasional break-ins, and even death threats—at times from government officials. In mid-2013, Emilio Lugo, editor of the Agoraguerrero news site, was forced to flee his home state of Guerrero after receiving threats for posting an article about the alleged murder of a federal police officer. Despite the many complaints about the efficacy of the Federal Mechanism for the Protection of Human Rights Defenders and Journalists, it was this governmental agency that assisted Lugo and his wife in relocating to a safer area.\(^6^5\)

As mentioned previously, the telecommunications act passed in July 2014 that enacts elements of the constitutional reform contains a number of worrisome provisions, including articles to provide


security agencies with blanket access to private data without need of a court order.66 Article 189 of the legislation requires telecoms to provide users’ locations and data to police, military, or intelligence agencies in real time, without a court order; Article 190 mandates that ISPs and mobile providers keep detailed records of user communications for two years; and Article 192 requires providers to provide this detailed information to security agencies without a court order. These provisions, along with others that stand to negatively impact user freedom and privacy, have received strong opposition from groups advocating for digital privacy and internet freedom rights.67

During the last few months of 2013, a number of editors and writers associated with online news outlets were subject to threats and police harassment. Silvia Nuñez Hernandez, editor of the online news portal AGN Veracruz, Carmen Olsen, editor of the Baja California-based news website Rosarito en La Noticia, and Jesus Issac Olmedo, editor of the online publication Reflexion en Linea, all reported police harassment in late 2013.68 Lydiette Carrion, an investigative reporter who writes about victims of violence, received death threats via Twitter in October 2013 in connection with an article she was writing about a musician who had disappeared. Carlos Lopez Lopez, a citizen who launched a Facebook page about civil opposition to an increase in prices of subway travel, also received threats on Twitter.69

Burglaries have also begun posing a threat to independent outlets. The digital newspaper e-Consulta, whose editor, reporters, and managers suffered a wave of arrests, defamation lawsuits, and kidnappings throughout 2012 and early 2013, suffered another 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.70 In March 2014, the house of Dario Ramirez, a director of the human rights and freedom of expression group ARTICLE 19, was burglarized. Ramirez’s computer and other documents were stolen during the raid, which occurred the evening before ARTICLE 19 was due to release a report regarding violence against journalists in Mexico.71

Violence against journalists has been a long trend in Mexico, and one that has steadily been spilling over into the realm of online media. In May 2014, Luz Maria Rivera, the director of the online news outlet El Mercurio, was assaulted in connection with her work. No suspect has been named, how-

ever Rivera noted that the attack was intended to drive her away from reporting. Although she has had to move multiple times due to fear of harm to her family, Ms. Rivera is dedicated to continuing her work as director of El Mercurio. 72 Additionally, Zoila Marquez Chiu, an online journalist with the news site Linea Informativa, was abducted in December 2013. In a rare turn, she was released and returned to her family after 17 days. To date, no suspects have been named.73

Between May 2013 and June 2014, Mexico was witness to at least one retaliatory murder for online journalism. Mario Ricardo Chávez Jorge, a columnist with El Ciudadano (The Citizen) and an active social media user who used his Twitter account (@laredroja) to post information about corruption among officials, was found dead in Tamaulipas in June 2013.74 The body of a woman who had been beheaded was also found near Chavez’s body.

Cyberattacks have also continued, and pose a growing threat to critical news sites. As of May 2013, Libre en el Sur, a local newspaper and online news website, had been victim to three cyberattacks in as many months.75 Libre en el Sur was again targeted later that month with an attack that affected linked Google and Twitter accounts and resulted in the deletion of 588 contacts from the editorial director’s Facebook account. The website of El Mañana de Nuevo Laredo, an important news outlet near the U.S.-Mexico border, suffered a distributed denial-of-service (DDoS) attack during the same month which forced the site to go offline for 20 minutes,76 the sixth in a series of cyberattacks the outlet experienced in 2013.77 In September 2013, another news site, Portal de Plumas Libres, reported a cyberattack preventing the website from being viewed for several hours. It is worth noting that each of these outlets is well known for its independence as well as its coverage of local crime and corruption.

---

Morocco

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>10</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>24</td>
<td>23</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>42</td>
<td>44</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 33 million

Internet Penetration 2013: 55 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Access to Lakome, an independent and investigative news site, was blocked on October 17, 2013, sparking local and international outrage over one of the first instances of state censorship in recent years (see Limits on Content).

- The blocking of Lakome, which came shortly after it had published controversial stories chronicling the royal pardoning of a convicted pedophile and extremists’ threats against the monarchy, has contributed to a slight increase in self-censorship among independent journalists (see Limits on Content).

- Ali Anouzla, editor-in-chief of the French-language version of Lakome, was arrested in September 2013 on charges of supporting and advocating terrorism in the context of an article he had written on jihadist threats in Morocco. He was apparently charged for providing a link to a Spanish news site, which in turn had embedded the jihadist YouTube video in question. He was released on bail in October and his trial has been repeatedly postponed (see Violations of User Rights).

- Two high school students were detained by police for one week in October 2013 in the city of Nador after a friend posted a photograph on Facebook of them kissing in front of their high school. All three juveniles were charged with violating public decency law, prompting a campaign in which activists staged kiss-ins and posted photos online (see Violations of User Rights).
Introduction

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. 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. This phenomenon has been furthered by the recent opening of the political system.

The most remarkable change in internet use among Moroccans is 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. By 2012, the sixth most visited site was Hespress, the most popular online news and information website in Morocco with estimated 400,000 unique visitors per day. Besides Hespress, now ranked fourth, the pan-Arabic sports website Kooora and two Moroccan classified ads sites, avito.ma and bikhir.ma, have also entered the top ten.

Social media has triggered a revival of the media’s traditional function as a watchdog, 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, for which voter turnout was 84 percent. These measures resulted in a lifting of all politically-motivated filtering.

The battle over the future of the internet as a public space for free political expression has stepped up over the past year. Authorities blocked websites (something not witnessed since 2009), threw a prominent journalist in jail, and strengthened an already existing atmosphere of self-censorship and fear. Revelations over the use of surveillance technology in democratic countries has served to justify its use in Morocco, where activists increasingly feel under threat and “owned” by the ruling regime. Optimists look to successful online campaigns, such as those to repeal the controversial rape law, to repeal the pardon of a convicted pedophile, and to release Lakome’s Ali Anouzla, as small but significant victories that can be replicated in the future. Many await the results of the U.S. call for a review of its surveillance policies and of Brazilian plans to tackle the issues on an international level.
level. However, pessimists believe they are losing the battle with the state, opting only to protect themselves through increased digital security skills to avoid surveillance. In the words of blogger Zineb Belmkaddem, “I don’t look at my smartphone the same way I did in the past. Instead of an empowering tool, I look at [my smartphone] as something that can be used against me. I do not possess all the information in it, it’s almost like a shared device, shared by me and my enemy, the entity that wants to take away my freedom.”

Obstacles to 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 just over 21 percent of the population in 2007 to 55 percent in 2013, according to the International Telecommunication Union (ITU). By end of 2012, roughly 2 in every 100 inhabitants possessed a fixed-broad subscription, or around 17.8 percent of all subscribers. The remaining 82.2 percent of all subscriptions are through 3G devices, including both data-only and voice-and-data connections. Morocco’s regulatory agency estimates the internet subscription annual growth rate to be 24 percent, with 4 million subscribers accounting for 12 percent of Morocco’s population. By December 2012, mobile phone penetration reached a rate of 119.7 percent, a rise of almost 20 percentage points compared to 2010. In 2012, Morocco doubled its bandwidth capability through the development of the Loukkos fiber-optic submarine cable.

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 37.1 percent of the overall population 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

---

5 Interviews with Aboubakr Jamai, Hisham Almiraat, Zineb Belmkaddem, IbnKafka and two other interviews conducted with online activists who want to remain anonymous from February 2013 and January 2014. Hereafter, Interviews with digital activists and online journalists.
Morocco

Index (IDI) ranks Morocco 89th, primarily due to a low adult literacy rate, gross secondary enrollment ratio, and gross tertiary enrollment ratio.12

The Moroccan government has undertaken several programs aimed at improving the country’s ICT sector. Launched in March 2005, the GENIE project (the French acronym for “Generalization of ICTs in Education”) aims to extend the use of ICTs throughout the public education system.13 Owing to positive results, another round of implementation was launched for the period of 2009–2013 to improve the training and professional development of teachers and encourage the adoption of ICTs by public school students. PACTE (French for “Program of Generalized Access to Telecommunications”) was launched in 2008 to provide 9,263 communities, or 2 million Moroccans, with telecoms services by 2010.14 Financing for the project came from Morocco’s Universal Service Fund for Telecommunications. The fund was created in 2005 using contributions from the three major telecoms operators: Maroc Telecom, Medi Telecom, and INWI. More recently, in 2009, authorities established the national strategy “Maroc Numérique 2013” (Digital Morocco 2013).15 The strategy aims to achieve nationwide access to high-speed internet and to develop e-government programs to bring the administration closer to its citizens, while encouraging small and medium-sized enterprises to adopt ICTs into their business practices. It has a budget of MAD 5.2 billion (around US$520 million).

Perhaps as a result of these efforts, internet use remains relatively affordable. For a 3G prepaid 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.

In the post-Arab Spring era, the government no longer blocks social media, 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.16

Service providers such as ISPs, cybercafes, and mobile phone companies do not face any major legal, regulatory, or economic obstacles.17 The allocation of digital resources, such as domain names

---

17 Interviews conducted on 20 February 2013, with Dr. Hamid Harroud and Dr. Tajjedine Rachdi, respectively director and former director of Information Technologies services of Al Akhawayn University in Ifrane.
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 43,354 registered
Moroccan domain names in 2012, the last year that figures were available.

The National Agency for the Regulation of Telecommunications (ANRT) is an independent
government body created in 1998 to regulate and liberalize the telecommunications sector. The
founding law of the ANRT considers 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 to
settle 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.

As mentioned, Maroc Telecom, Medi Telecom, and INWI are the three 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 ANRT granted licenses for
Medi Telecom and INWI. Medi Telecom is a private consortium led by Spain's Telefonica, 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.

Limits on Content

The past twelve months saw censorship issues once again make headlines in Morocco, as
independent news site Lakome was blocked in October 2013. In general, numerous obstacles to
access have resulted in online media not enjoying the same popularity and influence as television
and radio. For this reason, there are fewer instances of government intervention in the online
sphere, even if much more controversial statements are made on the web. Nonetheless, fears

18 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.
owned by Maroc Telecom.
20 Lois régissant la poste et les télécommunications (Laws governing the post and telecommunications), available online at
21 ANRT, Lois régissant la poste et les télécommunications.
BjörnWellenius and Carlo Maria Rossotto, “Introducing Telecommunications Competition through a Wireless License: Lessons
23 The State owns 30% of Maroc Telecom shares, 53% owned by the French telecoms company Vivendi; and 17% is public,
over intermediary liability and the prosecution of users have increased self-censorship, particularly regarding so-called “sacred” issues such as the monarchy and Islam.

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 2009.24

However, on October 17, 2013, in a move not seen since 2009, the Attorney General ordered the ANRT to block two news websites: the Arabic-language Lakome, along with its francophone version. Its editor-in-chief, Ali Anouzla, had been arrested one month earlier (See “Violations on User Rights”) for citing an article in the Spanish newspaper El Pais, which contained an embedded YouTube video attributed to Al Qaeda in the Islamic Maghreb (AQIM).25

Activists and observers believe Lakome was blocked for its critical stance towards the monarchy. Both the Arabic and the French versions of the site 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, France 24, 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.26

Some degree of uncertainty remains over how the site was blocked. On October 14, Anouzla issued a statement while in custody in a high security prison in Sale requesting the “temporary suspension” of the website Lakome, on grounds that he was unable to take legal responsibility for the site’s content while in custody. His lawyer shortly made the same request.27 However, the legality of the move was questioned by Aboubakr Jamai, editor-in-chief of the French-language version of the site. According to Jamai, Anouzla, as editor-in-chief of the Arabic site, did not possess ownership of either

25 The video entitled, “Morocco: Kingdom of Corruption and Despotism,” incites viewers to commit terrorism acts against the country.
26 Interview with Zineb Belmkaddem conducted on 15 January 2014. Belmkaddem is a Moroccan blogger, citizen journalist, 20th February activist.
of the sites and thus had no authority to take them offline. On October 18, one day after the two sites were blocked, Jamai created a mirror to the French site, which was blocked the same day.28

On January 9, 2014, Anouzla announced that he had submitted an official request to the ANRT to lift the blocking of Lakome.29 The ANRT responded by stating it required an order from the Attorney General, who had blocked the site.30 Anouzla has since said that the state’s security apparatus, rather than the ANRT or Attorney General, is behind the blocking. Access to the Arabic and the French sites was restored in January 2014, although the site is inactive.31 Anouzla stated that he may create a new website to pursue his journalistic work if unable to reactivate Lakome.32

The government maintains control over the online information landscape through a series of restrictive laws that can be manipulated to serve political purposes. 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 “Violations of User Rights”). The anti-terrorism bill33 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.”34 According to this law, legal liability rests jointly with the author, the site owner, and ISPs. Intermediaries must block or delete infringing content when made aware of it or upon receipt of a court order. 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, Mamfakinsh, and Febrayer, are hosted on servers outside of the country to avoid being shut down by the authorities.

Given the history of media repression in Morocco, many internet users and cyber activists engage in self-censorship. Harsh legal consequences for online speech ultimately deter freedom of expression.35 The arrest of Anouzla and the ensuing blocking of Lakome has strengthened the existing atmosphere of fear and self-censorship among online and traditional journalists.36 Popular websites now refrain from publishing content that crosses red lines. 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.37 In a state that punishes

---

28 Interview with Aboubakr Jamai conducted on 8 January 2014. Jamai is a Moroccan journalist who founded some of the most progressive magazines such as Le Journal Hebdomadaire and Assahifa al-Ousbouiya. In 2003, he was awarded the International Press Freedom Award of the Committee to Protect Journalists.

29 Interview with Aboubakr Jamai conducted on 8 January 2014.

30 Interview with Ali Anouzla conducted on 27 June 2014.


32 Interview with Ali Anouzla

33 The Anti-Terrorism Bill, 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.


35 Interviews with digital activists and online journalists.

36 Interviews with digital activists and online journalists.

37 Interview with Aboubakr Jamai conducted on 8 January 2014.
investigative reporting and whistleblowing, people with sensitive information tend to stay quiet to avoid possible retribution.

Activists and online opinion makers who openly criticize government policies receive personal attacks and derogatory comments from other users on social media. Numerous new accounts are created on Twitter and Facebook with the sole purpose to harass, intimidate and threaten activists. This army of paid users also mobilizes to write positive comments on media sites when news on the king’s activities is published. However, these comments often reflect a minority opinion on sites such as Hespress, where users can “like” or “dislike” comments. In many instances, positive comments on the king receive a rating of around -400, which indicates that at least 400 readers do not agree with the opinions expressed in the comment. However, it is very hard to link the regime to these groups of paid online users. Besides, as many activists recall from the experience of the February 20th Movement protests, there seems to be a lot of support for the king as a person from the public, especially with the situation in Egypt and Syria worsening.

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. 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 pro-government publications. 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. 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.

---

38 Interviews with digital activists and online journalists.
39 Bouziane Zaid, conference presentation, “The Internet, the Public Sphere and Morocco’s Democratic Transition,” The Arab-American Association of Communication Educators (AUSACE), Tangier, Morocco, 11-15 November 2013.
40 Interviews conducted with Almiraat, on 13 January 2014 and Ibn Kafka on 18 January 2014. Almiraat is the advocacy director for Global Voices, and a prominent digital activist in Morocco and abroad. Ibn Kafka is an anonymous Moroccan lawyer and a prominent blogger/activist.
41 Interview with Zineb Belmkaddem, conducted on 15 January 2014.
42 Interview with Aboubakr Jamai conducted on February 11, 2013.
43 Interview with Aboubakr Jamai conducted on February 11, 2013.
In a recent example of this, the Office Chérifien des Phosphates (OCP) and Caisse de Dépôt et de Gestion (CDG),\(^{45}\) 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 blogging services are freely accessible. ISPs are not known to limit bandwidth availability to discriminate on the basis of content.

Internet users take advantage of various social media tools to educate, organize, and mobilize people around a wide variety of issues. Facebook and mobile phones were used very effectively during the 2011 street protests. Facebook users grew by 490 percent from 860,000 to more than 5 million between 2009 and 2013 and the social network is the most visited website in the country.\(^{46}\) Moroccans effectively use blogs to disseminate their political views, reaching a wide online audience. Activists used mobile phones and cameras to present their version of street events in a bid to counter the censored, state-controlled news coverage.

The first widely covered instance of online activism occurred in 2008, when an amateur cameraman in the northern Morocco area of Targuist filmed traffic police officers taking bribes from drivers. The “Targuist Sniper” video circulated widely on YouTube and Facebook, resulting in a police investigation that led to the arrest of the several police officers. The video served as a model of cyber-activism against daily and mundane corruption in other Moroccan cities. Nevertheless, the effects on corruption and accountability remained short-term as the government eventually stopped responding to such videos.

One recent instance of online activism resulted in the overturning of a royal decree. On July 29, 2013, as is customary during the celebration of “Throne Day,” King Mohamed VI pardoned a number of prisoners. Among them was Daniel Fino Galván, a Spanish pedophile convicted of raping 11 children in the Moroccan city of Kenitra. He had served only 18 months of his 30-year sentence at the time of the pardon, after which he fled to Spain as a free citizen. The online news site Lakome broke the story on its Arabic and French websites and the news spread rapidly on social media. Demonstrations that took place in Rabat and Casablanca were met with a show force, leading to even more outrage.\(^{47}\) A Facebook page titled “Tous contre la libération de Daniel Fino Galván” [All against the freeing of Daniel Fino Galván] featured photographs of people from all over the world posing with messages in different languages calling for the capture of the convicted pedophile.\(^{48}\)

---

\(^{45}\) 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.


Another campaign of outrage and anger was launched on Twitter under the hashtag #DanielGate, which became one of the few globally trending hashtags to originate from Morocco.49

The campaign and ensuing protests led to the king withdrawing his pardon and instructing the justice minister to alert the Spanish authorities to arrest Galván. In an unprecedented move, the Royal Cabinet issued two press releases: the first to claim that the King has no knowledge of the case, leading to online cries asking what else the king has signed without his knowledge; the second revealed the canceling of the pardon and the opening of an investigation into the incident. The director general for prison administration was discharged from his duties as a result of the investigation.

Violations of User Rights

The Moroccan state continues to be strategic in its campaign to intimidate users and online journalists. Many prominent online activists remain free from prosecution, even if they continue to be harassed or intimidated through extralegal means.50 In general, activists often face trumped-up charges related to drug possession or disruption of public order. Several users were imprisoned during the coverage period for defaming the king or public officials. In the case that brought the heaviest international condemnation, online journalist and editor Ali Anouzla was arrested in September after publishing an article chronicling extremist threats against the government.

The Moroccan constitution of 2011 recognizes all Moroccan citizens as equals before the law.51 Article 25 provides that the constitution guarantees all citizens “freedom of opinion and expression in all its forms.” However, prior to the 2011 constitution, the Moroccan legislature adopted an array of laws that limited freedom of expression, such as the 2002 Press Code and the 2003 Anti-Terrorism Law. These provided legal sanctions against 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 27 of the 2011 constitution 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-2014, no new outcomes have been reached.

Although the 2011 constitution strengthened the judiciary as a separate branch of government, the judiciary system in Morocco is far from independent. The king chairs the High Council of Judicial

50 Reporters without Borders, “Hazards mount for freedom of information in Morocco.”
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.  

Article 38 of the Press Code 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 in 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 one case from October 2012, the head of the Council for the Moroccan Community Abroad sued the news portal Yabiladi for defamation over an article detailing his travel expenses.  

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. The draft was prepared by the Ministry of Trade, Investment and the Digital Economy. The draft law, consisting of 114 articles, aimed to reinforce the legislative framework of digital communication in Morocco and addressed e-government, e-marketing, e-commerce, digital security, and trust. 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 inciting violence, as well as any expression seen to undermine Islam, public policy or the privacy of individuals. Authorities were empowered to block any websites deemed offensive in this respect.  

The draft law triggered strong reactions from the public. For many online journalists and activists, the vagueness of laws such as proposed digital code and the press code are a danger to internet freedom. They argue that too many types of behavior could be considered abusive or immoral, depending on the interpretation and sometimes the mood of the judge. In response, a group of activists set out to crowdsource a new version of the digital code, critiquing aspects of the existing

---


57 Interviews with digital activists and online journalists.
The campaign seems to have paid off. The minister of industry, commerce, investment and digital economy announced in a tweet that he withdrew the draft bill on December 15, 2013, arguing that the digital code is so important that it necessitates broad consensus.

Some activists believe that the draft law might bring positive outcomes. They argue that the law is meant primarily to regulate e-commerce and digital security issues, and provisions in the draft law that are threatening to internet freedom already exist in the Press Code. Activists could consider this an opportunity and adopt a proactive stance to organize campaigns to include legislation that regulates surveillance. Once the law is there, citizens will have some legal protection, and this is better than having no protection at all.

Online journalists that push red lines when reporting on the monarchy face the threat of criminal prosecution. In the most publicized case, Ali Anouzla, journalist and editor-in-chief of the Arabic-language Lakome news site, was arrested on September 17, 2013, four days after publishing an article on extremists’ calls for holy war against the state. The article included a link to the site of Spanish news outlet El Pais, which in turn embedded the extremists’ video. Anouzla is a well-known journalist and his positions against terrorism are well-known to the public, prompting many to view the charges of providing “advocacy of acts amounting to terrorism offenses” and “providing assistance to perpetrators or accomplices of acts of terrorism” as an attempt to silence dissent. He was released on bail on October 25, 2013 and his trial has been continually postponed.

On October 4, 2013, two high school students were arrested and detained in the city of Nador for one week after a friend posted a photograph on Facebook of them kissing in front of their high school. All three juveniles were charged with violating public decency law. The arrest triggered a campaign in which activists staged kiss-ins and posted kissing photos online. The couple appeared in court on November 22, 2013 and was discharged with a warning.

Two users were serving jail sentences during the coverage period for their online activities. Walid Bahoumane, an 18-year-old student, was sentenced to 18 months in prison in March 2012 for “attacking the nation’s sacred values” after he allegedly ridiculed King Mohamed VI through a cartoon of the king he posted on Facebook. Abdelsamad Haydour is a 25-year-old activist who was sentenced to three years in prison in February 2012 over a video in which he criticized the king.

---

58 See the crowdsourced document at https://docs.google.com/document/d/13XBnZ546vKO4aNA-cktKLoC8nFLVho0pR6c6-FADY3o/edit.
60 Interviews conducted with Almiraat, on 13 January 2014 and Ibn Kafka on 18 January 2014.
62 Interview with Aboubakr Jamai.
Morocco

while conversing with another citizen on the street. The conversation was filmed by a bystander and uploaded to YouTube. The case represents yet another startling violation of freedom of expression, ostensibly protected in the new constitution. Also in jail is Mohamed Attaoui, an online journalist and environmentalist. Attaoui was arrested on January 21, 2013 and later sentenced to 10 months in jail for posting videos of public officials engaging in illegal tree felling.

Ali Lmrabet, a well-known progressive journalist, continues to be the target of constant violent and nonviolent harassment by the security and intelligence services in the northern city of Tetouan. Lmrabet runs the website Demainonline, which is openly critical of the monarchy and politicians in Morocco. However, in 2005 he was banned from publishing in Morocco for a period of 10 years, and some believe the state has not arrested him given the negative media coverage it may generate. The ban has so far only been applied to print media.

After spending one year in jail for “insulting the police” in a music video posted on YouTube, Mouad Belghouat, known as al-Haqed or “the spiteful,” continues to be harassed by the police. He was arrested on May 18 in Casablanca while entering a soccer stadium and handed a four-month jail sentence and US$ 1,200 fine for “scalping tickets to a soccer match, public drunkenness, and assaulting a police officer.” Details over the veracity of the accusations are difficult to obtain, but according to some witnesses, the police explicitly targeted Belghouat.

While users are punished for content they post online, Moroccan citizens can create websites and write for blogs without any registration requirements imposed by the government. 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 an ID. Today, customers are asked for a copy of the ID. However, street vendors and other non-affiliated sales outlets continue to provide SIM cards without IDs. Free access with anonymity is currently still available, but this slight change is significant.

Some activists have voiced their suspicion that telecommunications companies may be cooperating with government authorities by passing on swathes of user data to security forces to conduct widespread surveillance. There are suspicions that Maroc Telecom, through its subsidiary in Mali, performed intelligence gathering for French authorities prior to the recent military intervention in

72 Interviews conducted on 29 March 2013 with Dr. Fouad Abbou, full professor of computer Science and Telecommunications and Dr. Hamid Harroud, director of the Information Technologies Services of Al Akhawayn University in Ifrane.
that country by French troops. Many activists have questioned whether the company performs similar actions in Morocco.

In December 2011, Reflets, a French news site, published an investigation on the purchase of spyware from the French company Amesys. The article refers to an investigation carried out by journalists from the Wall Street Journal who found that Amesys 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 spent time in the country training government personnel for the use of such sophisticated spyware. The software, called Pop Corn, is used to monitor emails, Skype conversations, and other kinds of encrypted materials.

Moroccan activists identified surveillance as the most dangerous instrument in the hands of the regime. Many feel they have lost all sense of privacy and do not know the extent of the state’s capabilities. 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 Mamfakinsh and one of the leaders of the February 20th Movement, explained, the state’s capacity to own and reconstruct your own personal story, based on surveillance and monitoring, allows authorities to “assassinate your character and use your own information to hurt you.” According to 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.” Activists demand that the state must be transparent with regards to surveillance. They demand that the state informs the public on who is conducting surveillance on whom and for what reason.

However, some activists doubt if the state has the capabilities, skilled human resources, to conduct large-scale surveillance and to use that information to incriminate activists. One can easily notice the low level of computer equipment and the human competencies in the average police station in Morocco. With the exception of the secret and intelligence services and their workforce, who are highly trained and equipped, the rest of the police force have the bare minimum qualifications to fight street crime. The state monitors suspected terrorists and Western Sahara separatists and that is very likely to be their first priority. They may target the activists who they perceive as threatening, but these must be low in numbers.

In addition to surveillance and malware attacks, online news portals that express dissenting voices are subject to continuous cyberattacks. Activists have admitted that, in order to maintain a functional news website, they must pay a substantial amount of money to maintain guards against cyberattacks. Almiraat stated that in July 2011 his website was subjected to a cyberattack by a

76 Interview with Zineb Belmkaddem conducted on 15 January 2014.
77 Interviews with digital activists and online journalists.
sophisticated computer virus. 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 a company in Milan, Italy. The virus downloads itself and hides among files, reading keystrokes and taking control of the keyboard and webcam at will.

The company refused to disclose its list of clients and there is no direct evidence that can link the state to such a purchase. However, prices for this type of software range in the hundreds of thousands of dollars, thereby ruling out private individuals. “There is only circumstantial evidence,” Almiraat said in an interview, “but it leads to one and only one conclusion; the state is the only entity that has the financial power and the political motivation to target websites who publish dissenting content.”

---

78 Interview with Hisham Almiraat, conducted 13 February, 2013.
Myanmar

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>20</td>
<td>19</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>26</td>
<td>25</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>62</td>
<td>60</td>
</tr>
</tbody>
</table>

Population: 53.3 million
Internet Penetration 2013: 1.2 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

* 0=most free, 100=least free

Key Developments: May 2013 – May 2014

- In March, Norway’s Telenor activated Myanmar’s first independent link to the international internet (see Obstacles to Access).

- Mobile penetration increased slightly under a program to distribute affordable SIM cards, but remains among the world’s lowest (see Obstacles to Access).

- The October 2013 Telecommunications Law reduced, but did not abolish, prison terms for online activity (see Violations of User Rights).

- Democratic Voice of Burma video journalist Zaw Pe was sentenced in April 2014 to a one-year prison term in relation to his online reporting (see Violations of User Rights).

- Government officials pressured independent online media to alter advertisements and threatened to deny interviews (see Limits on Content).
Introduction

Telecommunications is becoming one of the most dynamic sectors in Myanmar’s gradual transition from military rule to democracy.1 In June 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. In October, the government passed a Telecommunications Law drafted with input from the international community.2 Under the new framework, Norway’s Telenor Group established the country’s first independent connection to the international internet in March 2014. Qatar’s Ooredoo introduced mobile phone service in much of the country in August.

The government of former military leader President Thein Sein officially ended media censorship in 2012, and internet freedom improved in 2013. The practices of the old regime, however, endure. Authorities employ legal, administrative, and other sanctions to influence content, and some clauses in the Telecommunications Law may allow censorship and surveillance.3 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. In January 2014, the government granted YTP a license to provide broader telecommunication services, further tilting a playing field that smaller players argue is already skewed. Plans to privatize the state-owned Myanmar Post Telecommunication (MPT) have not materialized since they were announced in 2012.

The telecommunications minister was dismissed amid an antigraft probe in early 2013. Yet despite official commitments to good governance, military-owned conglomerates still appear to be manipulating the market. The military-owned Myanmar Economic Corporation (MEC) began distributing data-enabled SIM cards for US$1.50 by means of a ballot in April 2013. Access to a cell phone cost up to $200 in 2012, so affordable connections represent major progress. Yet the distribution system was mired in corruption allegations, and cards resold on the black market for over $100.4 Mobile penetration increased, but remains one of the lowest in the world, with just one phone for every two households. The internet also lacks bandwidth to support the surge in online activity.5 Users said connection quality actually deteriorated in the past year as government and private sector services, including banking and commerce, came online. Inadequate infrastructure and electricity shortfalls are major challenges to overcome before access can expand.

---

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.


3 Interviews with three journalists and two web developers in Rangoon, October 2013; Daily Eleven, August 31. News citations without links refer to hard copy editions.

4 Daily Eleven, August 28 and 29.

Online communication reflected political polarization developed in advance of 2015 elections. Opposition leader and Nobel Peace Prize laureate Aung San Suu Kyi of the National League for Democracy (NLD) party now serves in parliament.\(^6\) But she is barred from running for president in elections scheduled for 2015 under a clause in the constitution which excludes her for having family members who are foreign nationals—her children and late husband. The 2008 clause was drafted with her in mind, her supporters believe, and digital campaigns were waged by those who would amend the clause and those who would maintain it.\(^7\) The influence of rising religious nationalism also increased online. The government has maintained discriminatory policies against ethnic minorities like the Muslim Rohingya,\(^8\) 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.

### Obstacles to Access

The Telecommunications Law passed on October 12, 2013, providing a foundation for the privatization of the industry. In March 2014, the Norway-based Telenor Group established an independent connection to the international internet.\(^9\)

Yet poor infrastructure and widespread poverty continue to limit citizens’ internet access and usage. The number of internet users has notably increased over the past four years, but remains a fraction of the population. The International Telecommunication Union (ITU) estimated internet penetration at 1.2 percent in 2013, up from 1.07 percent in 2012.\(^10\)

Private internet connections are prohibitively expensive, though there is significant regional variation. The one-time installation cost of home broadband access ranged from $58 to $500 in early 2013, down from $530 to $588 the previous year, depending on speed and connection method. Prices continued to fall during the coverage period.\(^11\) However, since Myanmar’s gross domestic product was just $913 per capita in 2013, these costs keep personal internet access far out of reach for the majority.\(^12\)

More people can access the internet via mobile phone. MPT has offered mobile phones since the 1990s, but charged from $2,000 to $5,000. The price dropped to $200 in 2012. In 2012, officials

---


\(^11\) The MPT adjusted pricing from $58 to $50 for ADSL installation, plus an additional $100 modem fee, $50 annual charge, and monthly data plan. Plans ranged from $17 for 512 Kbps to $66 for 2 Mbps; YTP charged $100, plus a $50 modem fee, $60 annual charge, and the cost of monthly service. $60 for 512Kbps to $100 for 1Mbps; Redlink still charges $450 for installation, plus additional costs. An annual fee $60 for its Wi-Fi service. Its monthly fees vary from $30, $55 and $90 for 512Kbps, 1Mbps and 2Mbps of download speeds respectively.

blocked a private company's initiative to sell more affordable SIM cards, but in 2013 it allowed MEC and MPT to distribute a finite number of SIM cards per month for less than $2 each. Slow speeds and constant disruptions continue to drive up mobile internet prices, particularly since November 2013. Users reported needing from one to five minutes to load a single web page. A regular mobile internet user might spend MMK 10,000 to 20,000 ($10 to $20) per month, while those who rely on it for business spend from 30,000 to 50,000 ($30 to $50). SIM cards operating the CDMA 800 MHz radio frequency experienced worse connectivity problems than GSM phones on a 2G network. Many SMS messages were never delivered or arrived after long delays, though they are automatically charged on sending.

The system for distributing these cheap SIM cards was a gift to corrupt officials and black market racketeers. Rather than make them available through service providers, users were directed to local government offices, where they were asked to submit household registration, ID, and two photos for the opportunity to enter a draw for one of the new cards. A US$1.50 SIM was soon worth much more on the black market. In September 2013, the Rangoon regional government set up a committee to monitor and supervise the draw, but has yet to have a noticeable effect.

The system threatened to perpetuate the urban-rural digital divide. The MPT sold more than half its SIM cards in Rangoon, and users in remote areas that lack the infrastructure to support frequent phone usage met with an automatic financial penalty when their credit expired within two months. Failure to purchase additional credit within 15 days of expiration led to disconnection. Power outages, service interruptions, and lack of transmission towers made the conditions onerous, and the company later announced it would revise them.

Overall, there were over 1.2 million internet users on mobile phones in July 2013, according to MPT, and 7 million mobile phones operating in Myanmar by December 2013. Teledensity in 2014 was 27 percent, a 10-percent increase over the previous year. Despite the increase, this still averages just one mobile phone per two households. In April 2014, one year after affordable SIM cards were introduced, official statistics said 4.25 million had been sold.

Until this year, the Ministry of Communications and Information Technology (MCIT) controlled the country’s international connection to the internet through two main ISPs, the state-owned Myanmar Post Telecommunication (MPT), and the military-linked Yatanarpon Teleport (YTP). Redlink, SkyNet, and other FTTH providers operate under YTP.

---

13 Myanmar Internet Journal, author interviews. Prior to the publication of this report, Myanmar Internet Journal was in the process of transferring online content from http://myanmarinternetjournal.com to a new URL, at http://www.internetjournal.media. Articles consulted between May 2013 and May 2014 had yet to be made available at the time of publication.
14 Myanmar Internet Journal, author interviews.
15 Myanmar Internet Journal, author interviews.
17 There are over 8.7 million households in Myanmar. See, http://www.7daynewsjournal.com/article/11806.
18 http://myanmarinternetjournal.com/content/12035.
19 Many still refer to the Ministry, formerly responsible for Communications, Posts and Telegraphs, by its old abbreviation MPT.
In 2012, the government announced plans to liberalize its telecom sector and invite foreign investment. In June 2013, the government awarded international licenses to Norway’s Telenor and Qatar’s Ooredoo, allowing them to offer services and infrastructure alongside local firms. The tender and selection processes were widely applauded as fair and transparent. After the Telecommunications Law was enacted in October 2013, operator licenses for the two companies followed in January 2014. Both subcontracted other international companies to build infrastructure. MPT also plans to cooperate with Telenor, Ooredoo, and other operators to expand the telecoms network and build over 80,000 transmission towers across the country.

Telenor said it would pay $500 million for a 15-year license in addition to expenditure on network construction, and expects to break even of its investment, which could peak at $1 billion, in three years. In February 2014 the CEO of Telenor Myanmar said in February the company would sell 2 and 3G SIM cards for $1.50 each, with coverage expanding to 90 percent of the country in five years. Telenor also said it is in the process of hiring 3,000 employees, setting up a Telenor Myanmar Academy for training them, and invited distribution representatives and retail stores to join its network. Ooredoo pledged to invest $15 billion to develop Myanmar’s telecom sector and said it would roll out a network within six months, aiming for 97 percent coverage in five years. The firm will sell a 3G SIM card for MMK 1,500 kyat ($1.50). At a Rangoon press conference in August 2013, Ooredoo announced its plan to hire over 30,000 employees, 99 per cent of them local. However, training is urgently needed to fulfil employment goals. Local candidates who applied for jobs at ICT firms in 2013, even technical graduates, were underqualified and limited to administrative positions.

To compete with Telenor and Ooredoo, MCIT officials said MPT would transform from a state-owned to a public firm. Local news reports said MPT invited Orange and Vodafone, two leading telecommunication companies that did not win the operating licenses, to enter into a private partnership. YTP, now 49 percent private-owned, began transforming into a public company in 2012, though the process has been opaque. The other 51 percent remains government-controlled. What’s more, military-linked entities own most of the public holdings, while the company’s transfer of state-owned capital to a new, public firm lacked transparency. The newly-constituted firm has 23 directors, including many accused of cronyism in connection with the junta, further tainting the transition. Some, such as Asia World’s Tun Myint Naing, remain subject to United States and European Union sanctions for its involvement in illicit drug business. On January 30, 2014, the government granted YTP

---


26 Interview with three graduates from Technical Institute and Computer University, and four graduates of other majors including Accounting, and English, Rangoon, August and September 2013.

27 See, http://www.ft.com/intl/cms/s/0/b8dc836-3d14-11e3-86ef-00144feab7de.html#axzz2tX5IfF8A.


29 Daily Eleven, September 6, and November 27, 2013.
a telecommunications license, making it the fourth service provider after state-owned MPT, Telenor and Ooredoo.\textsuperscript{30}

Despite progress, military-owned conglomerates continue to skew the telecommunications playing field. In December 2013, the Central Bank granted military-owned Inwa Bank a mobile banking permit, an idea first mooted by Telenor and Ooredoo in June.\textsuperscript{31} In September, the head of Telenor Myanmar even advised the government to draw up robust regulations and to open the market to “as many players as possible,” rather than specifying individual banks to launch mobile services.\textsuperscript{32} However, observers said Inwa benefitted from a special relationship with the Central Bank to obtain permission ahead of rival companies, though Central Bank officials said the military institution was simply better prepared, and that all private banks applying for the licenses would be treated fairly. Meanwhile, Lieutenant General Wai Lwin, chairman of Inwa, urged other private banks to join Inwa’s platform instead of setting up their own mobile banking networks.

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.\textsuperscript{33} Low bandwidth is largely responsible for the congestion experienced by local internet users, especially during peak afternoon hours. Officials said bandwidth would be increased before the Southeast Asian Games, a biennial regional sporting event in December 2013.\textsuperscript{34} That upgrade did not take place until February 2014, and still fell short of demand.\textsuperscript{35} Both MPT and MED bought vehicles equipped with mobile transmission systems to reduce congestion.\textsuperscript{36} MPT in partnership with other providers spent several hundred thousand dollars to provide 4G service. However, attendees complained that the connectivity did not improve even near stadiums.\textsuperscript{37}

Bandwidth was particularly limited between July and September 2013 after a fault damaged the SEA-ME-WE 3 cable south of the Irrawaddy delta.\textsuperscript{38} The internet was completely interrupted for a few hours, but disruptions continued while repairs were made. All users were affected, and the slow connections had a particular impact on financial transactions and local industry.\textsuperscript{39} No government-initiated service interruptions were documented during the coverage period of this report. However, Clause 77 of the October 2013 Telecommunications Law created a legal framework for possible future interventions, authorizing the MCIT to direct any private enterprise “to suspend a telecommunication service, restrict specific forms of communication, jam or intercept any commu-

\begin{itemize}
\item \textsuperscript{32} See, \url{http://www.economist.com/news/finance-and-economics/21586841-mobile-phones-may-regenerate-countrys-withered-banking-system-leapfrog-spotting}.
\item \textsuperscript{33} See, \url{http://www.irrawaddy.org/investment/fiber-fix-brings-Myanmars-internet-back-up-to-speed.html}.
\item \textsuperscript{34} See, \url{http://www.irrawaddy.org/Myanmar/Myanmars-internet-receive-high-capacity-upgrade.html}.
\item \textsuperscript{35} \textit{The Voice}, January 30 2014.
\item \textsuperscript{36} See, \url{http://www.7daynewsjournal.com/article/12968}.
\item \textsuperscript{37} See, \url{http://www.7daynewsjournal.com/article/12907}.
\item \textsuperscript{38} See, \url{http://consult-myanmar.com/2013/07/25/myanmar-internet-down-to-crawl-speed-as-sea-me-we-undersea-cable goes-for-repair/}.
\item \textsuperscript{39} See, \url{http://myanmarinternetjournal.com/content/11930}.
\end{itemize}
FREEDOM ON THE NET 2014

Myanmar

tion, hand over telecommunication equipment, or take temporary control of any telecommunication equipment.”

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. 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 industry. By-law drafts on licenses, competition, and networking were presented to the Attorney General’s Office in March 2014. However, the by-law governing the regulator, expected in February 2014, was delayed due to a translation error, as it was drafted in English.

Limits on Content

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. While digital content was not censored during the coverage period, sensitive political and social topics were less visible.

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-2014. While content remained available and new readers were more likely to encounter it than they were in the past, authorities made a concerted effort to exclude certain topics from mainstream discourse. Independent publications, while freer than they were, rely on state-owned newspapers New Light of Myanmar and The Mirror to advertise their content to the much wider readership they built up with the junta’s official sanction when the censorship remained in place. In late 2013 and early 2014, independent publications including the monthly Human Rights and Democracy journal, Pae Tin Than (Echo) weekly, and Mawkun (Annals) journal—which publish online and print editions—reported state-owned newspapers removing references to human rights, government corruption, and sensitive social issues such as premarital cohabitation from advertisements the independent outlets had

40 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.

purchased to publicize their content. Advertising requires pre-publication approval from government officials.42

The *Irrawaddy* weekly came under particular pressure after it launched a print version of its online Burmese-language edition in early 2014, a significant step for an outlet that was formerly exile-run. *The Mirror* soon refused to run *Irrawaddy* advertisements citing lack of space, but also told them to “tone down” political headlines. Government officials separately told *Irrawaddy* editors that an illustration of the president published in the second issue was inappropriate, and the Ministry of Information (MOI) insisted they change the spelling of their brand, which they have used for two decades since they launched in English.43 Though their publishing license was approved with the spelling “Irrawaddy,” they were instructed to adopt “Ayeyarwady” in keeping with the official spellings imposed by the military junta in 1989. When they refused, authorities indicated their access to the government for media interviews would be limited if they fail to comply.

Traditional journalists also faced sanctions in reprisal for their coverage. Min Naing Soe, the editor of the weekly *Ludu Pon Yait* (Public Image) was fired after authorities accused the journal of spreading politically radical views. Other weeklies such as *Eleven Media*, *Thandaw Sint* (Herald) and *True News*—many of which also have an online presence—received official or informal warnings for their reporting on corruption and military-related issues.44 Information officials shortened the duration of select foreign journalist visas from three months to one in February, and sought more detailed personal details and itinerary from applicants, focusing on media organizations that covered anti-Muslim violence.45 An edition of *Time* magazine covering the violence was banned in June 2013, though it remained accessible online.46

In this climate, self-censorship remains common online, though topics considered off-limits have evolved during liberalization. Internet users are reluctant to discuss past abuses for fear of jeopardizing the political opening. In December 2013, police said they were investigating a former police officer who leaked old interrogation records on his pseudonymous Facebook account. His supporters said the leak was in the public interest, because they illustrated that individuals with political connections broke the law with impunity under the junta.47

The persecuted Rohingya minority also lack representation online, and individuals or news outlets that provide even neutral coverage of religious tensions are accused of anti-Burmese bias.48 Some progovernment blogs, such as *Myanmar Express* and *OppositEye*, actively manipulate online commentary to launch smear campaigns against Muslims or the political opposition. In May 2014, a radical group of Buddhist monks named *Ma-Ba-Tha* (the Association of Protection of Race and Religion) launched an anti-Ooredoo campaign based on the telecom giant’s roots in a Muslim country. The

---


43 Interview with the editor and publisher of The Irrawaddy Publication Group. Interview with other journalists working in Myanmar.

44 Interviews with an editor from Weekly Eleven Media, and four other journalists working for affected media outlets.


group announced a boycott,\textsuperscript{49} denouncing anyone working for Ooredoo, or using their services, as a traitor. The government did not intervene.\textsuperscript{50}

Social media and communication apps including Viber, Tango, Friendfinder, and Google+ are freely available. Facebook is the most popular, 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. For some users frustrated at 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.\textsuperscript{51}

Ethnic Burman internet users also spread racially-charged comments across social media platforms throughout the coverage period.\textsuperscript{52} A Buddhist monk named Wirathu used Facebook and YouTube to spread vitriol against Muslims, who he accused of raping Burmese girls.\textsuperscript{53} A Facebook page in his name has thousands of supporters. Wirathu's 969 movement galvanized Buddhist nationalists in Arakan state and elsewhere to protest against allowing the Rohingya minority to register their ethnic identity in a 2014 census sponsored by the United Nations Population Fund.\textsuperscript{54} In March 2014, the government conceded and said it would reject census respondents identifying themselves as Rohingya.\textsuperscript{55} Nationalists also campaigned extensively during the coverage period to restrict interfaith marriage, a proposal submitted to parliament in May 2014.\textsuperscript{56} The 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.\textsuperscript{57}

Counter campaigns also had some success. An opposition initiative to amend Clause 59F is gaining currency online. The Panzagar or “Flower Speech” movement opposes the spread of anti-Muslim sentiment and has gained media attention and popular support.\textsuperscript{58} 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.\textsuperscript{59} In late 2013, activists mobilized public protests when the government proposed raising the price of electricity. Public outrage on issues such as land grabbing and corruption often find their first expression on the web.

\textsuperscript{58} See, https://www.facebook.com/panzagar.
Besides employing online tools for social and political mobilization, users have organized gatherings such as BarCamp meetings in Rangoon and several other cities to share ICT-related expertise. In January 2014, MIDO and the U.S. Embassy held a two-day technology TechCamp in Rangoon, where technology and civil society experts discussed how digital tools can address real world challenges.

Violations of User Rights

The October 2013 Telecommunications Law transformed the industry, but failed to repeal harsh punishments for political dissent on electronic media. Fears that these could be abused to repress government critics grew as traditional media journalists were arrested during the year. Digital video journalist Zaw Pe was sentenced to a year in prison in relation to an interview he conducted in 2012. Hackers targeted the Eleven Media news website for “slandering the government.”

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. But media and rights activists pointed to many shortcomings. Notably, the law failed to repeal the notorious Electronic Transaction Law (ETL) of 2004, which has routinely been used to criminalize internet activism. Instead, parliament amended the ETL, reducing but not eliminating possible jail sentences for ill-defined online actions.

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.”

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.”

60 Local ICT firms and foreign companies such as Ericsson attended BarCamp held at the Technological University (Thanlyin) in August 2013 and recruited potential employees from students and other participants. Daily Eleven, August 10 2013.


He also proposed improving a law regulating e-commerce and drafting one to combat cybercrime, though a possible timeframe for doing so is unclear.  

Dozens of political prisoners formerly jailed for electronic activities remain free since 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.  

The year 2014 saw a sharp decline in press freedom in Myanmar which affected at least one reporter with a digital platform. Zaw Pe, a journalist working for the online, formerly exile-run news outlet Democratic Voice of Burma (DVB), was sentenced in April 2014 to two one-year prison sentences, to be served simultaneously, for trespassing and disturbing an official. An appeals court released him in July but failed to acquit him. The charge was based on a 2012 video interview that took place during business hours at an education department office in the central Magwe region, where the journalist was investigating alleged funding irregularities. Zaw Pe was among several DVB video journalists jailed for independent digital reporting under the junta, and international and local civil society groups condemned his 2014 trial. At least five other journalists were detained during the coverage period of this report. After May 2014, nine traditional media practitioners were sentenced to prison terms ranging from two to seven years; separately, one was fatally shot in military custody.

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 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 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

---

66 Myanmar Internet Journal, author interviews.
67 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.
asked information officials for clarification about interception rules and procedures. Ooredoo told journalists it will prevent any wiretapping of its phone networks.73

Phishing attacks targeting activists appeared to decline during the coverage period. However, Eleven Media Group's news website was defaced in June 2013 by hackers who accused the outlet of slandering the government. Eleven Media said nationalist Facebook pages shared news of the attack immediately after it happened, but that internet protocol (IP) addresses associated with the attack were based in China and Russia.74

Nigeria

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Obstacles to Access (0-25)</strong></td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td><strong>Limits on Content (0-35)</strong></td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td><strong>Violations of User Rights (0-40)</strong></td>
<td>13</td>
<td>15</td>
</tr>
<tr>
<td><strong>TOTAL</strong> (0-100)</td>
<td>31</td>
<td>33</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 173.6 million

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Penetration 2013:</td>
<td>38 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>Yes</td>
</tr>
<tr>
<td>Press Freedom 2014 Status:</td>
<td>Partly Free</td>
</tr>
</tbody>
</table>

Key Developments: May 2013 – May 2014

- Mobile phone services were shutdown in three northern states from May to December 2013 following the announcement of emergency rule in the region as part of a military strategy against the Boko Haram terrorist group (see **Obstacles to Access**).

- In November 2013, progovernment trolls were accused of blocking links to articles posted on the Facebook page of the well-known investigative online news outlet, *Premium Times* (see **Limits on Content**).

- Two individuals were arrested for posts on social media platforms: one in October 2013 for allegedly criticizing the governor of Bayelsa state on his Facebook page; the other in March 2014 for live-tweeting an incident involving Boko Haram militants and the State Secret Service (see **Violations of User Rights**).

- The regulator announced a new directive in October 2013 requiring cybercafes to register customers and maintain an up-to-date database of subscribers (see **Violations of User Rights**).

- Suspicions of government surveillance increased following a November 2013 report about the installation of a mass surveillance system and revelations that the 2014 budget contained various earmarks for the purchase of specialized surveillance equipment (see **Violations of User Rights**).
Introduction

In 2014, access to the internet and other information and communications technologies (ICTs) continued to spread across the country due to the growth of mobile phone usage and data services. Public and private sector investments in ICT infrastructure and increased competition between service providers also played a key role. In May 2013, the Nigerian government approved a National Broadband Plan that aims to increase Nigeria’s broadband penetration five-fold by 2018. Nonetheless, the government deliberately impeded access to mobile phone networks in the northeastern states of Borno, Adamawa, and Yobe as part of a military strategy against the Boko Haram terrorist group in May 2013, imposing emergency rule and cutting off telecommunications in the region through December.

Compared to the traditional media sphere in Nigeria, online media is relatively free from restrictions, and no blocking or filtering of online content was reported during the coverage period. Self-censorship has noticeably declined since the January 2012 Occupy Nigeria protests, and people now freely discuss issues that were previously unpopular or taboo, such as gay rights, in spite of the controversial anti-homosexuality law that passed in February 2014. Hashtag activism through social media campaigns such as #BringBackOurGirls in 2014 become a highly influential tool for citizens to draw widespread attention to important issues and demand government accountability.

Nevertheless, observers suspected the government of trying to manipulate the online information landscape, pointing to the growing number of suspicious Twitter users who actively attack critical voices as evidence. 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 articles’ links as abusive. The news outlet also reported experiencing a massive DDoS attack against its website in January 2014.

Arrests of internet users increased in the past year, with two individuals arrested for posts on social media platforms. One individual was arrested in October 2013 for allegedly criticizing the governor of Bayelsa state on his Facebook page. The other was arrested in March 2014 for live-tweeting an incident involving Boko Haram militants and the State Secret Service.

Meanwhile, Nigerian users became increasingly suspicious of online surveillance during the coverage period, even as the government continued its push to make ICT tools more available to citizens. Various legislative proposals were drafted in 2013 and 2014 that involve the interception of user communications, while the regulator announced a new directive in October 2013 requiring cybercafes to register customers and maintain an up-to-date database of subscribers. Suspicions of government intentions to monitor ICTs increased further following a November 2013 news report revealing the government’s contract with the Israel-based Elbit Systems to install a mass surveillance system by 2015. The publicly available summary of the federal government’s 2014 budget proposal also included various earmarks for the procurement of specialized surveillance equipment.

---

Nigeria

Obstacles to Access

The internet in Nigeria has continued to spread rapidly, particularly with the proliferation of mobile phone data and Fixed Wireless Access (FWA) services. In 2013, internet penetration stood at 38 percent, up from 33 percent in 2012, according to the International Telecommunication Union (ITU). Mobile phone teledensity also increased from 86 percent in May 2013 to 92 percent in April 2014, as reported by the Nigerian Communications Commission (NCC), while the ITU indicated a mobile phone penetration rate of 73 percent in 2013, up from 67 percent in 2012.

Increasing access to the internet has been driven in large part by internet-enabled mobile handsets that provide affordable bundled data services to mobile subscribers. For example, as of January 2014, BlackBerry service packages cost as low as US$17 a month, an option that attracts many young Nigerians. Competition, helped by the Mobile Number Portability initiative launched in April 2013, has forced service providers to offer cheaper plans based on time (daily, weekly, or monthly) or use (for social media or messaging). According to the NCC's Internet Subscriber Data reports, there were about 66 million active internet subscriptions on GSM and CDMA networks in Nigeria in April 2014, while the ITU noted a mobile-broadband penetration rate of 10 percent in 2013. Nevertheless, the quality of service remains poor, with users frequently complaining about their inability to enjoy seamless data services.

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. Internet speeds are still slow, however, averaging 1.9 Mbps (compared to a global average of 3.9 Mbps), according to May 2014 data from Akamai's "State of the Internet" report. In addition, Nigeria's broadband adoption (characterized by connection speeds greater than 4 Mbps) was about 5 percent, while the country's narrowband adoption (connection speed below 256 kbps) was 4 percent. Although many providers use the word "broadband" in their promotional materials, in practice there is limited broadband service.

---

2 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.
5 International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2013."
available in Nigeria. A mere 0.1 percent of Nigerians had access to fixed-broadband internet in 2013, representing just over 15,000 subscriptions.12

The ICT market in Nigeria has expanded considerably over the past decade, with the number of licensed ISPs rising from 18 in 2000 to 156 (55 of which have licenses in need of renewal13) by the end of 2013. There are also 11 FWA providers,14 and five GSM mobile phone operators that provide internet access to their subscribers.15 Nevertheless, the growth of ISPs and FWA providers has slowed in recent years with the rise in mobile access. As of September 2013, the four privately-owned GSM companies—MTN, Globacom, Airtel, and Etisalat—had a total of over 118 million subscribers among them.16

Recognizing the importance of ICTs for economic development, the communication ministry released the National Broadband Plan (2013-2018) in May 2013, which was approved by the president shortly thereafter.17 In accordance with the National Broadband Plan, the telecommunications regulator announced that it planned to auction a 2.5 GHz frequency spectrum by March 201418 and license seven Infrastructure Companies (InfraCos) by December 2014.19

In the meantime, access to ICTs in Nigeria is characterized by a large urban-rural divide. According to a May 2014 Gallup survey of 4,000 adults across the country, 34 percent of urban Nigerians had used the internet in the last week, compared to 22 percent of rural Nigerians.20 Similarly, 89 percent of urban Nigerians reported owning a mobile phone, compared to 79 percent of rural Nigerians, though the gap between urban and rural mobile phone owners is narrowing. In 2012, the same Gallup survey in Nigeria found that 70 percent of rural Nigerians owned a mobile phone, compared to 85 percent of urban Nigerians.

High costs are another major impediment to internet access. While increased competition among service providers has made the cost of access more affordable, the country’s median annual per capita income stood at US$493 in 2013.21 FWA services cost an average of US$63 per month, while the price for internet use in a cybercafe can cost about US$0.63 per hour. As technologies expand, however, prices are continuing to decrease; in 2013, for example, the average cost of a GSM plan cost US$0.05 per megabyte of data, compared to US$1 per megabyte in 2011.

---

13 55 Internet service providers have expired licenses 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 December 31, 2013, http://bit.ly/1dO6p5e.
In addition to cost, power cuts continued to disrupt service and access, with many users reporting the need to use private generators to stay online during outages. The country’s electricity supply saw major disruptions in 2013, and Nigeria is still reportedly the largest importer of private power generators in Africa, despite the country’s status as an oil-rich country. To address the country’s inadequate power supply, the federal government took an unprecedented step in November 2013 and handed over its state monopoly of the power sector to private investors. The private sector is expected to revitalize the nation’s power supply, though the impact of this endeavor will take years to come into effect.

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 via mobile devices.

The government deliberately cut off access to mobile phone networks in the northeastern states of Borno, Adamawa, and Yobe in May 2013, ostensibly as part of a military strategy against the Boko Haram terrorist group in the region. Residents complained of hardship due to the lack of telecommunications services and argued that the imposed shutdown did not help the government stop the terrorist threat. Instead, the shutdown at times put citizens in harm’s way. In September, for example, residents travelling to another city in search of mobile phone connectivity were reportedly ambushed and killed by Boko Haram militants. Phone lines were restored months later in December but were cut off again in March 2014 for about 20 hours.

Internet services are managed by the 2003 Nigerian Telecommunications Act, which vests regulatory responsibilities 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. 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 challenges in their operations due to competition from larger ISPs and investor focus on the mobile sector. Meanwhile, the process of issuing GSM licenses has been regarded as transparent. Unlike similar auctions that have been subject to political

---

interference, most stakeholders found the first and subsequent GSM license auctions to be fair, as friends of prominent politicians, who are usually recipients of such licenses, lost out in the process.

**Limits on Content**

No blocking or filtering of online content was reported during the coverage period, though progovernment trolls were suspected of manipulating the information landscape on social media networks. Hashtag activism became a highly influential tool for citizens to draw widespread attention to important issues and demand government accountability.

Online media is generally free from restrictions in Nigeria, and to date, the authorities have not carried out any blocking or filtering of content, mainly due to the complex nature of Nigeria’s internet infrastructure, which makes it difficult to carry out systematic filtering or censorship. Some ISPs have been known to block access when users infringe on laws by downloading copyrighted content, but this has often been done to manage network traffic rather than to protect intellectual property. Nonetheless, Blue Coat’s PacketShaper 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’s monitoring and filtering equipment in authoritarian countries such as China, Bahrain, and Russia.

The video-sharing website YouTube, social-networking site Facebook, microblogging application Twitter, and various international blog-hosting services are freely available and among the most popular websites in the country. According to the website rating company Alexa, the ten most popular websites in Nigeria in 2013 were Google, Google Nigeria, Facebook, Yahoo, YouTube, Blogspot, Nairaland, Twitter, the Vanguard and LinkedIn. Five other Nigerian websites were cited in the top 20, including LindaIkeji, a gossip news site; Punch newspaper; and Jumia, an eCommerce website.

Meanwhile, websites, blogs, and online commentators are generally divided among those with antigovernment, progovernment, and neutral leanings. Web commentary is generally balanced, with online commentators having more discussions on socioeconomic issues than polarized debates. Online self-censorship has declined notably in the past few years, and people now freely discuss issues that were previously unpopular or taboo, such as gay rights, in spite of the repressive anti-homosexuality law passed in February 2014. Criticism of the government on social media has also increased, as have responses from government representatives.

Government efforts to manipulate online content are sporadic in Nigeria, though observers have noted a sharp increase in the volume of progovernment responses to citizen comments on social media.

---

31 Discussion between a Freedom House consultant and Citizen Lab.
32 As of December 2013, there were over eleven million Facebook users. Based on Facebook advertising data accessed by author on December 31, 2013.
media in recent years. In addition, the growing number of suspicious Twitter users who 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 articles’ links as abusive. Efforts to unblock the Premium Times’ links succeeded months later in January 2014.34

Another case of suspected progovernment manipulation surfaced in March 2014 when it was discovered that the president’s special adviser on new media, Reno Omokri, had tried to plant a story in the media with the pseudonym Wendell Simlin.35 According to reports, Simlin had sent an email to journalists with a Microsoft Word attachment that accused the suspended governor of the Central Bank, Lamido Sanusi, of sponsoring the terrorism group Boko Haram, shortly after Sanusi accused the government of corruption, which led to his subsequent suspension.36 Digital activists linked the random Wendell Simlin to the president's new media adviser when Reno Omokri’s name was found listed as the email’s author in the attached document’s properties.

In the past few years, high-level government officials have made numerous statements calling for a clampdown on social media,37 ostensibly as a response to the growing influence of critical commentary on the internet, which drew reactions from citizens who viewed these statements as signs of impending online censorship.38 While the government denied any intent to restrict social media,39 it seems determined to create its own social media tools, as indicated by Nigeria’s 2013 budget proposal40 in which the information ministry had made provisions to spend NGN 100 million (US$623,000) for “developing social media platforms and networking with other platforms.”41 The information ministry proposed NGN 50 million (US$312,500) for the same project in 2014, along with an additional NGN 7 million (US$43,750) for the “integration of social media platform collaboration including secured WAN.”42

There has also been some government interference in the economic aspects of online news publishing, though overt incidents have not been recorded in the past few years. In 2011, the

---

leading critical online newspaper, 234Next, folded in part due to a refusal to provide advertising by government or progovernment businesses. As the country gears up for national elections in 2015, government patronage is still evident and reputed to be the largest source of business contracts that companies depend on for financial sustainability.

Nonetheless, Nigeria is home to a diverse blogosphere, with entertainment blogs drawing the most readers and a growing number of Nigerians blogging about their personal lives or social issues. Blogs have gradually emerged as an important platform for discussion and a source of reliable news for many users, providing a space for lengthy debate among online commentators. Readers often leave comments on popular news-oriented blogs to express frustration with societal issues. The Nigerian blogosphere includes both expatriates and locally-based writers, and popular platforms on which Nigerian bloggers interact and learn from one another include Global Voices, Blogger, and WordPress. The president's Facebook page is a major platform on which citizens comment on public issues, and Twitter plays a prominent role in debates around events as they happen, with government ministers often hosting Twitter chats with the public.\(^\text{43}\) The formal chats were less frequent in 2013 and 2014, but ministers continued to use social media directly, employing media aides to comment on issues that concern them.

In addition, ICTs are playing an increasingly important role in mobilizing people for protests and providing updates on unfolding events. Citizens are more active on social media and increasingly believe that campaigns initiated on social media can lead to change. Online citizen activism in Nigeria was particularly evident in 2013-2014, as demonstrated by an incident involving allegations of corruption against a serving minister. On October 28, 2013, Punch newspaper published an editorial that criticized the president for not acting on the widespread calls for the dismissal of aviation minister Stella Oduah, who had allegedly used public funds to purchase bullet-proof vehicles for her personal use.\(^\text{44}\) The allegations elicited nationwide outrage to the story, especially on social media where “Oduah-gate” became a popular topic. While many assumed that the scandal would join the growing list of unresolved corruption cases in Nigeria, social media users kept the discussion alive, which played a large part in the government’s decision to indict Oduah in January 2014.\(^\text{45}\)

In another showcase of online activism in Nigeria, the governor of Edo State was compelled to act upon criticisms against him on social media when a video of him insulting a woman selling wares on the roadside was posted online in November 2013. The video, which depicted the governor telling the woman to “go and die” in response to her plea against his inspection of her sale of allegedly illegal wares, became popular on social media and sparked an online campaign on the subject of human dignity. The ensuing online discussions and fundraising for the widow led the governor to issue a formal apology, invite the woman to his office, offer her a job, and donate NGN 2 million to her family—gestures that were all publicized on social media.\(^\text{46}\)

The most notable social media activism in 2014 was spurred by the horrific kidnapping of over 200


schoolgirls by the Boko Haram terrorist group in April. The hashtag #BringBackOurGirls became an international social media campaign that put a spotlight on the Nigerian government and its inadequate efforts to take action. Foreign governments eventually pledged support to help locate the girls, but as of this report’s writing in mid-2014, the rescue mission was still ongoing.

Nonetheless, the #BringBackOurGirls campaign illustrated how hashtag activism has become a highly influential tool for citizens to draw widespread attention to important issues and demand government accountability. In April 2014, one hashtag campaign, #FreeCiaxon, launched following the disappearance of a man who had live-tweeted the scene of an attempted jailbreak in Abuja (using the Twitter handle @ciaxon), led to the man’s eventual release by the authorities who had covertly detained him (see “Violations of User Rights”).

Violations of User Rights

Various legislative proposals were drafted in 2013 and 2014 that involve the interception of user communications, while the regulator announced a new directive in October 2013 requiring cybercafes to register customers and maintain an up-to-date database of subscribers. Two individuals were arrested for posts on social media platforms: one in October 2013 for allegedly criticizing the governor of Bayelsa state on his Facebook page; the other in March 2014 for live-tweeting an incident involving Boko Haram militants and the State Secret Service. Suspicions of government intentions to monitor ICTs increased further following a November 2013 news report revealing the government’s efforts to install a mass surveillance system by 2015.

Nigeria’s 1999 constitution guarantees freedom of expression and of the press, and the lack of internet-specific legislation has generally fostered an open environment for online activities. Nonetheless, the country’s legal framework was revised in 2011 to reflect the use of new media technologies through Section 84(1) of the 2011 Evidence Act, which provides for the admission of statements in documents produced by computers and electronic signatures as evidence in court. Libel also remains a criminal offense in Nigeria, 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. Meanwhile, the implementation of Sharia (or Islamic) law in 12 northern states has not affected internet freedom to date.

There are currently no laws in Nigeria that specifically restrict online speech, though a draft bill on electronic transactions and fraud detection proposed in 2011 did include a provision that sought to punish online speech regarded as “false information that could threaten the security of the country or that is capable of inciting the general public against the government through electronic message” with heavy fines, up to seven years in prison, or both. Following public backlash against the draconian provision, especially on social media, the senate announced that the controversial clause would be deleted from the proposed bill in December 2013.
In addition to national legislative initiatives, state government officials in Nigeria have made efforts to restrict freedom of expression within their jurisdictions. In March 2013, for example, the governor of the southern state of Bayelsa, Seriake Dickson, introduced a bill to the state assembly that aimed to criminalize “rumor mongering” and the spread of false information.\(^5\) While the bill is still under consideration as of mid-2014, it has not deterred Governor Dickson from cracking down against alleged rumor-mongering online.

Notably, on October 26, 2013, known businessman Tonye Okio was arrested in Abuja, blindfolded, and driven to Bayelsa State by the Nigeria Police’s Special Investigation Bureau for allegedly criticizing the governor of Bayelsa on his Facebook page.\(^5\) The police also reportedly seized Okio’s electronic gadgets and deleted the critical posts about the Bayelsa governor from his Facebook account. He was held for 10 days without trial and subsequently granted bail under politically-motivated conditions that were “impossible” to meet, requiring an agent of the complainant to stand as Okio’s surety for the bail.\(^5\) Okio later was released on January 22, 2014 after spending three months in prison.\(^4\) He was reportedly one of several victims of the Bayelsa state government’s proposed rumor mongering law.\(^5\)

In another notable incident during the coverage period, a Twitter user (@ciaxon) was covertly detained in March 2014 after he live-tweeted a series of photos depicting the attempted escape of suspected Boko Haram members who were being held at a State Secret Service (SSS) facility.\(^5\) His photos were picked up by media outlets covering the story, leading to suspicions that the SSS was behind his disappearance.\(^5\) Large-scale protests initiated by the hashtag campaign, #FreeCiaxon, elicited international attention and ultimately led to his release 12 days later.\(^5\)

SIM card registration requirements instituted in June 2009 impose restrictions on users’ rights to anonymous communication.\(^5\) In addition, a new directive announced by the regulator in October 2013 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,”

---


Nigeria

as part of the government’s efforts to combat cybercrime. As of mid-2014, there have been no reports that the new registration requirements have been enforced, and it remains unclear whether the authorities need a court order to gain access to customer information from cybercafe records.

In February 2013, the NCC introduced a new draft Lawful Interception of Communications Regulation. Still under discussion as of mid-2014, the regulation was criticized for potentially infringing on the constitutional right to privacy, in addition to a lack of safeguards against abuse or opportunities for redress, and unclear supervisory and reporting provisions. If implemented, the bill 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 “provide the National Security Adviser and the State Security Service with the key, code or access to the Protected or Encrypted Communication.”

Meanwhile, throughout 2013 and 2014, the National Assembly began discussing other proposed laws that also address the subject of lawful interception, such as the Oral and Written Communications Tracking Bill, Regulation of Telecommunication Facilities to Support Investigations Bill, Electronic Fraud Prohibition and Electronic Transfer of Funds Crime Bill, the Interception of Communications Bill, and the Cybercrime Bill. Though most of the draft bills—all still under discussion as of mid-2014—require security agencies to obtain a court order before they can conduct surveillance activities, warrants are generally easy to obtain in the context of Nigeria’s nominally independent judiciary.

Meanwhile, ISPs are currently required 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, according to the “Guidelines for the Provision of Internet Service” published by the NCC. 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.

---

64 Nigeria Communications Commission, “Draft Lawful Interception of Communication Regulations.”
68 “Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission,” 3.
Thus far, the Nigerian security services have not appeared to proactively monitor internet and mobile phone communications, but many online journalists have long suspected that they are being monitored by the state, and the government’s recent acquisition of mass surveillance equipment has deepened these suspicions. In April 2013, the online newspaper *Premium Times* published a news report revealing that the federal government had awarded a secret contract to Israel-based Elbit Systems to help monitor internet communications in Nigeria. A civil society organization working on ICT Policy, Paradigm Initiative Nigeria, made a Freedom of Information (FOI) request on the contract in May 2013, but to no avail, eliciting a lawsuit that was subsequently dismissed by a judge in a widely criticized ruling. In August 2013, a local anti-corruption organization accused the judge of bias based on his apparent pattern of opposition to rights-focused suits.

Evidence of government plans to implement a surveillance system was further corroborated by publicly available details of Nigeria’s 2013 budget, in which the Office of the National Security Adviser requested US$61 million for a “wise intelligence network harvest analyzer system, open source internet monitoring system, personal internet surveillance system.” 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. As of mid-2014, the extent to which such surveillance systems have been implemented has yet to be established, though in November 2013, *Premium Times* reported that Elbit Systems staff was in Nigeria and working to complete the mass surveillance system within two years.

Meanwhile, in the publicly available summary of the federal government’s 2014 budget proposal, the Directorate of State Security Services listed plans to spend NGN 415 million (US$2.6 million) on a “Data Retention System,” NGN 359 million (US$2.2 million) on a “GSM Passive Off-the-air Interception System,” and NGN 350 million (US$2.2 million) on a “Strontium Sky Diligent Recon System.” The Office of the National Security Adviser similarly proposed NGN 11 billion (US$68.8 million)—more than its total budget on mass surveillance equipment in 2013—on its ongoing “Enhanced and Specialized Security Equipment, Gadgets and Services” project, and another NGN 5.2 billion on an unexplained “Security Program for Federal Courts.” While the exact purpose of these technologies is still unclear, the planned 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 Boko Haram threat.

Online journalists and internet users have not been subject to significant extralegal intimidation or threats for their activities, though the state is known to target journalists in the traditional media with arbitrary and extralegal measures to suppress political criticism. The Nigerian authorities have a

---

69 Ogala Emmanuel, “EXCLUSIVE: Jonathan awards $40 Million Contract.”


74 Ogala Emmanuel, “EXCLUSIVE: Elbit Systems officials arrive; begin installation of $40 million Internet Spy facility for Nigeria.”

Nigeria

history of arresting and intimidating traditional media workers, and at least ten journalists have been killed in connection with their work since 1998.\textsuperscript{76} In addition, there is a culture of impunity for crimes against media workers.

Cyberattacks have increased in Nigeria, though most of the attacks are against government websites and carried out by the Naija Cyber Hacktivists,\textsuperscript{77} a group that has claimed responsibility for almost all cyberattacks to date. One DDoS attack against an independent news outlet known for its critical coverage of the government, \textit{Premium Times}, was reported in January 2014.\textsuperscript{78}


\textsuperscript{78} “PREMIUM TIMES survives major cyber attack,” Premium Times, January 5, 2014, \url{http://bit.ly/1ducg5f}.
Pakistan

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>27</td>
<td>29</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>67</td>
<td>69</td>
</tr>
</tbody>
</table>

Population: 190.7 million

- Internet Penetration 2013: 11 percent
- Social Media/ICT Apps Blocked: Yes
- Political/Social Content Blocked: Yes
- Bloggers/ICT Users Arrested: Yes
- Press Freedom 2014 Status: Not Free

* 0=most free, 100=least free

Key Developments: May 2013 – May 2014

- Four women were brutally killed for using mobile technology in rural areas of Pakistan (see Violations of User Rights).
- In April 2014, a judge in Punjab sentenced a Christian couple to death for blasphemy in relation to a text message they deny sending (see Violations of User Rights).
- Lawyer Rashid Rehman was shot dead on May 7 after receiving threats for representing a professor jailed on charge of committing blasphemy on Facebook (see Violations of User Rights).
- YouTube has been blocked since September 2012 while officials jockey to systematize control over the platform (see Limits on Content).
- Authorities newly blocked film details referencing Baloch independence and a gay community website (see Limits on Content).
- Citizen Lab researchers found Netsweeper technology automatically blocking political and social content on Pakistan’s largest ISP (see Limits on Content).
- The Pakistan Protection Ordinance 2013 categorized unspecified “internet offenses” as terrorism, with suspects subject to arbitrary detention (see Violations of User Rights).
Pakistan

Introduction

Pakistan saw a democratic change of power in May 2013, when citizens ousted the leftist Pakistan People’s Party led by former President Asif Ali Zardari in favor of the conservative Pakistan Muslim League–Nawaz party under Prime Minister Nawaz Sharif. The newly elected government became the latest in a line of both military and civilian authorities to restrict information and communications technologies (ICTs). Human rights monitors accused them of bolstering military and police powers, instead of addressing past abuses.¹

Though framed as necessary to combat terrorism and preserve Islam, censorship in Pakistan continues to reflect political motives or the influence of religious extremists. Religion also influenced a series of incidents which eroded user rights during the coverage period. At least four women were violently killed in rural areas of Pakistan for using digital technology, which their communities condemned as immoral. In the central province of Punjab, several people faced blasphemy charges based on SMS or Facebook messages, including one couple in their forties who were sentenced to the death penalty, though the phone they were accused of using was not in their possession. A lawyer defending another digital blasphemy suspect was fatally shot in his office for accepting the case.

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. In June 2013, researchers at the Canada-based Citizen Lab documented a Canadian company, Netsweeper, already filtering political and social content on the Pakistan Telecommunication Company Limited (PTCL) network. Besides being Pakistan’s largest ISP, the government-owned PTCL controls a large percentage of the country’s internet backbone.

Other efforts could cement government control of Pakistan’s internet. Civil society groups said a pending 2014 cybercrimes act would disproportionately criminalize some online offences and give ill-defined and overbroad powers to a government-appointed authority. The downsides of this proposal were in stark relief during the coverage period of this report when another government-appointed body, the Pakistan Telecommunication Authority, was left without a chair or even a membership for several months thanks to a combination of disorganization, political power struggles, and allegations of wrongdoing. The disruption contributed to the late introduction of 3G and 4G mobile internet services, which, pending since 2011, were finally offered in May 2014.

Obstacles to Access

Internet penetration in Pakistan stood at 11 percent in 2013, according to the International Telecommunication Union.\(^2\) A local report put the figure at 16 percent mid-year.\(^3\) Mobile penetration was at 70 percent.\(^4\) Low literacy, difficult economic conditions, and cultural resistance have limited the proliferation of information and communication technologies (ICTs) in Pakistan.\(^5\) While the cost of internet use has fallen considerably in the last few years,\(^6\) and cost around US$12 a month for a broadband package, access remains out of reach for the majority of people in Pakistan, and most users go online at their workplace or school.

The internet service providers (ISPs) association listed 50 operational in Pakistan in 2014.\(^7\) Fourteen offer high-speed broadband.\(^8\) 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.\(^9\)

Broadband subscriptions, based on DSL—which uses existing telephone networks—or wireless Wi-Max technology, are concentrated in urban areas. The majority government-owned Pakistan Telecommunication Company Limited (PTCL) controls 60 percent of the broadband market.\(^10\) It also owns the Pakistan Internet Exchange (PIE), having three main nodes in Karachi, Islamabad, and Lahore, with 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.\(^11\) PTCL controls access to the undersea fiber-optic cables SEA-ME-WE 3 and SEA-ME-WE 4, named for connecting South-East Asia, the Middle East, and Western Europe, and I-ME-WE, between India, the Middle East and Western Europe.\(^12\) In the past, damage to these cables disrupted half of the country’s connections.\(^13\)

Most remote areas lack broadband, and a large number of users depend on slow dial-up connections or EDGE, an early mobile internet technology. Meaningful online activity like multimedia training can be challenging. Conflict-stricken areas like Khyber Pakhtunkhwa (formerly North West Frontier Province) and the Federally Administered Tribal Areas (FATA) have significantly poorer internet

---


\(^4\) International Telecommunication Union, “Mobile-cellular Telephone Subscriptions, 2000-2013.”


\(^7\) http://www.ispak.pk/.

\(^8\) http://www.pta.gov.pk/annual-reports/annreport2013_1.pdf.


Pakistan as a whole faced electricity shortfalls throughout 2013 and early 2014, resulting in outages lasting several hours across the country, lasting as long as 20 hours a day in rural areas. A 2006 Universal Service Fund promised to establish telecommunications centers in rural areas with more than 5,000 inhabitants, among other initiatives. However, contracts for building the centers were cancelled without public explanation and are being re-auctioned.

Administrative hurdles long stymied the introduction of an internet-capable 3G mobile network. First mooted in 2011, 3G and 4G auctions remain stalled due to bureaucratic processes. The National Assembly said the PTA under former head Mohammed Yaseen had mishandled the initial auction of 3G licenses, and cancelled them in late 2012. Yaseen’s term expired that year, and the Lahore High Court annulled the appointment of his successor or Farooq Awan on technical grounds in early 2013, even as terms expired for the body’s other two members. A new chair, Ismail Shah, was appointed nine months later. In December, Shah announced plans to auction 3G and 4G licenses by March 2014. Bids were accepted in April, and mobile operators began offering faster service in May, though coverage is limited to a few urban centers.

Mobile operators 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.

Telecommunications providers in Pakistan also suffer from periodic government-mandated service disruptions. During 2012 Pakistan Day celebrations, mobile service was cut “to implement national security policy” in the southern province of Balochistan, where a conflict between Baloch nationalists and state security forces or antiseparatist militias has persisted since 1948. At least one local official denied security concerns and characterized the shutdown as routine maintenance, but many Baloch people saw the move as discriminatory. Urban areas nationwide saw similar interventions in 2012 and 2013, and in the past year, the new government disappointed businesses and civil society groups by maintaining the same tactics. Mobile service in 80 cities around the country was interrupted during a religious procession on November 14, 2013. To thwart sectarian violence, network

---

services were also suspended in major urban cities during a religious event celebrating the birth of the Prophet Muhammad on January 14, 2014.26

Internet cafes do not require a license to operate, and opening one is relatively easy.27 This freedom is occasionally threatened at the local level. In 2012, the provincial cabinet in Punjab approved a law which some analysts said would oblige cafe owners to register their businesses, among other requirements.28 Provincial elections in May 2013 reshuffled the local administration and the law was never implemented. In October 2013, the Khyber Pakhtunkhwa provincial government ordered local police to keep records of cybercafe users and data, and recommended cafes install hidden cameras to monitor people sending threatening emails.29

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.30 The prime minister appoints the chair and members of the three-person authority, which reports to the Ministry of Information Technology and Telecommunication.31 The repeated failure to make these appointments in the past year further undermined the PTA’s reputation.

Limits on Content

YouTube remained blocked since ISPs blocked it on government orders in September 2012. The new administration said Google would launch a local version of the site which would be required to censor objectionable content, but the status of this plan—and the extent of Google’s cooperation—remains in doubt. In the meantime, even as officials cited the absence of automated filtering technology in Pakistan as a rationale for maintaining the block, the Canadian company Netsweeper was documented implementing filters on the government-controlled ISP, PTCL. While civil society opposition partially succeeded in staving off additional blocks on VoIP applications and the movie website IMDb during the coverage period, the lack of transparency surrounding this secretive and far more systematic censorship bodes ill for their ability to keep limits on content in check going forward.

Since January 2003, the government of Pakistan has censored some online content, and the system for doing so is becoming increasingly sophisticated, though it lacks an adequate legislative framework.32 A variety of government agencies are involved, but the PTA is the primary authority. The Inter-Ministerial Committee for the Evaluation of Web Sites (IMCEW) established in 2006 in-

---

clcludes PTA and governmental representatives, as well as “men from the Ministry of Religious Affairs, the Inter-Services Intelligence, and Military Intelligence.”

A range of overbroad provisions in the 1996 Pakistan Telecommunications Act support censorship for the protection of national security or religious reasons. Authors 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 antistate content. Critics believe these issues can serve as a 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. A satirical music video about military generals was replaced on video-sharing site Vimeo by a page telling viewers it was “prohibited” within Pakistan in mid-2013. Besides blocking, the PTA issues takedown orders involving banned content. Twitter removed allegedly blasphemous posts at the government’s request in 2014, though restored at least some on review.

Historically, the PTA has directed ISPs and backbone providers to implement manual blocks on individual URLs or IP addresses, their compliance ensured by licensing conditions. Since 2012, successive administrations have sought to introduce technical filtering. The National ICT Research and Development Fund initially requested companies develop nationwide blocking technology to “handle a block list of up to 50 million URLs,” though the status of that project was left in doubt after widespread civil society protests. News reports in 2013 and 2014 said PTA and government officials were still pursuing filtering solutions.

34 Article 19, “Legal Analysis – Pakistan.”
38 Article 23 of PTA Act 1996 says “Where a licensee contravenes any provision of this Act or the rules made thereunder or any term or condition of the license, the Authority may by a written notice require the licensee to show cause within thirty days as to why an enforcement order may not be issued.

34 Article 19, “Legal Analysis – Pakistan.”
38 Article 23 of PTA Act 1996 says “Where a licensee contravenes any provision of this Act or the rules made thereunder or any term or condition of the license, the Authority may by a written notice require the licensee to show cause within thirty days as to why an enforcement order may not be issued.
In June 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. In addition to using Netsweeper technology to block websites, ISPs also use other less-transparent methods, such as DNS tampering,” Citizen Lab noted. The report highlighted the lack of transparency and accountability surrounding censorship in Pakistan as it becomes more advanced.

The same lack of transparency extends to the content affected by censorship, which is often inconsistent based on location or across ISPs. 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.

Censorship targeting pornography can affect access to legitimate content like Scarleteen, a U.S.-based sex education website for teenagers. In May 2013, Pakistani Twitter users reported they could not access the social media platform Tumblr, which Netsweeper filters frequently flag for pornographic content. In September 2013, the PTA confirmed that it had ordered a block on Queer Pakistan, the country’s first ever website for the queer, transgender and bisexual community to communicate anonymously, just months after its launch. 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.

Blocks increased in early 2014. Net users around the country reported different sites were temporarily inaccessible, including the UK-based Guardian newspaper, Gawker, Storify, and some online games. The blocks were never explained, though hundreds of social media users complained.

Blocking frequently targets social media and communication apps, and different religious groups persistently pressure the Pakistani courts to ban Facebook completely. Groups and individuals affiliated with political and religious causes have also filed court petitions against YouTube. In September 2012, the information ministry instituted a site-wide block on YouTube in response to the anti-Islamic video “The Innocence of Muslims.” Another 20,000 websites were also blocked, either for

43 Citizen Lab, “O Pakistan.”
44 DNS tampering intercepts the user’s request to visit a functioning website and returns an error message.
48 Citizen Lab, “O Pakistan.”
featuring the video or for hosting material that the PTA characterized as “objectionable.” YouTube was unblocked very briefly in December 2012 until a broadcast journalist demonstrated that the offensive clip was still available.

Civil society groups protested against the YouTube ban, and in 2013, petitioners challenged it in the high courts in Lahore and Peshawar. Hearings in both cases are ongoing. In Lahore, the deliberations centered on the possibility of localizing YouTube, so it would become subject to domestic content restrictions. 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 December, Anusha Rehman said the PTA was drafting an ordinance protecting Google from legal responsibility if internet users uploaded blasphemous content. The ordinance has not been made public and its scope is not known. Once it is complete, however, “Google will easily be able to block blasphemous content on the request of the Pakistan government,” Rehman said, though it was not clear if the company had agreed to do so. YouTube remained inaccessible through May 2014.

Political dissent and secessionist movements in areas including Balochistan and Sindh province, where a Sindhi nationalist movement advocates for political divisions along ethnic lines, is among the nation’s most systematically censored content. On November 19, 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 on Freedom,” a fictional depiction of Pakistani security agencies abducting Baloch separatists. In 2014, IMDb was largely accessible again, yet the page documenting “The Line on Freedom” was still blocked. Pages relating to the movie are also inaccessible on other sites, including Vimeo.

While most other social networking and blog hosting platforms were available and widely used throughout 2013 and early 2014, VoIP applications came under threat in Sindh during an antiterror campaign. On October 3, the local administration—run by the now-opposition Pakistan People’s Party—requested the federal government implement a three-month localized ban on services such as

---

57 Sumaira Jajja, “YouTube ban.”
Pakistan

as Skype, WhatsApp, Viber, and Tango to limit their use by “criminal elements.”64 The plan—which was blocked by federal authorities and never publicly implemented—triggered protests among civil society and internet users, and locals called it discriminatory.65 Voice calls on Viber became briefly inaccessible nationwide the same month, but it was not clear if the service had been intentionally disrupted.66

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 go interact online undetected and access blocked websites—to curb communication between terrorists.68 International and civil society organizations in Pakistan protested,69 and the tools remain widely used to access YouTube.70 Two of the best-known services, Spotflux and HotSpot VPN, became inaccessible in January 2014, and Spotflux said the government had actively blocked its services.71 Both were later restored.

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.72 ICTs, particularly mobile phones, promote social mobilization. The 2010 floods in Pakistan, for example, inspired many Pakistani citizens and members of the diaspora to mobilize and raise funds online.73 Nevertheless, most online commentators exercise a degree of self-censorship when writing on topics such as religion, blasphemy, separatist movements, and women’s and LGBT rights.

In May 2013, reports of election rigging spread via Facebook and Twitter, prompting traditional media coverage.74 Voters from around the major urban cities reported incidents live from their polling stations. While many failed to turn in to anything tangible, a plethora of users in Karachi reported

70 The VPN blocking in Pakistan is taking place under the section 5(2)(b) of PTA Act 1996 and the same provision was used as justification for the “Monitoring and Reconciliation of Telephony Traffic Regulation under which the current VPN blocking is happening. See, http://www.pta.gov.pk/media/monitoring_telephony_traffic_reg_070510.pdf.
ballot-rigging using videos and photos, then mounted a successful offline protest. In response, the Election Commission called a recount in over 40 polling stations in the city’s largest constituency.75

Violations of User Rights

User rights experience a steep decline during the coverage period, mostly stemming from religious intolerance. Four women were killed by male family members in rural areas of Pakistan, one for possessing a mobile phone, and three for featuring in a video circulating on community mobile networks. Three men were murdered for being gay by a man who used social media to identify their sexual orientation. Blasphemy charges for digital content spiked in Punjab, where a judge sentenced a Christian couple to the death penalty for an allegedly blasphemous text message they denied sending, and a lawyer was shot dead for his work defending another user in a blasphemy case related to Facebook. Problematic laws were also being debated during the coverage period, including the Pakistan Protection Ordinance, which listed unspecified “internet offenses” as acts of terror.

Article 19 of the Pakistani constitution establishes freedom of speech as a fundamental right, although it is subject to several restrictions.76 Pakistan became a signatory to the International Covenant on Civil and Political Rights in 2010.77

A controversial counterterrorism law, the Pakistan Protection Ordinance, was promulgated by President Mamnoon Hussain on October 31, 2013. An executive order subject to parliamentary review, it was amended in January 2014 and approved by the National Assembly in April, when opposition politicians staged a walk-out in protest. Freedom of expression advocates were concerned by the draft’s inclusion of unspecified “internet offenses” as terrorist acts, with suspects potentially subject to arbitrary arrest or extrajudicial execution.78 The Senate did not approve the ordinance, and the National Assembly subsequently approved a resolution to extend it for 120 days, effective at the end of the coverage period on May 22, 2014. With some reformulation, it was passed as the Pakistan Protection Act in August.79 One news report said the interior ministry issued a separate order putting the ordinance in effect from December 5, 2013.

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 it in June 2014, outside the coverage period of this report.80

---

Pakistan

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.81

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 have involved electronic media.

Blasphemy charges for digital content saw an alarming spike in the central province of Punjab in 2013 and 2014. On May 7, 2014, Rashid Rehman, the defense lawyer in another digital blasphemy case in Punjab was shot dead in his office by unidentified assailants after receiving multiple death threats in relation to the case, including in court from lawyers for the prosecution. He was defending Junaid Hafeez, an English professor and former Fulbright scholar jailed since 2013 for alleged blasphemy on Facebook, a charge based on an unsupported accusation by a religious group.82

In April 2014, the Pakistan Today newspaper reported that a judge had found a Christian couple guilty of sending a blasphemous text message to local Muslims, and sentenced them to the death penalty. Their defense lawyer said the phone they were accused of using had been lost. Police detained Shafqat Emmanuel, a disabled man, and his wife Shagufta Kausar, a cleaner, along with their four children, in June 2013. Their lawyer told the newspaper the sentence was not based on concrete evidence, but “a receipt of a cellular company on which Shagufta’s national identity card number was written against the number.”83 They are appealing the sentence, which is unlikely to be enforced.84

In November 2013, a religious leader in Punjab accused an unemployed 25-year-old man in his village of blasphemy for allegedly sharing objectionable content on Facebook.85 No details of the alleged post were publicized. The man was arrested, and no trial was subsequently reported, though he remained in detention, according to a journalist familiar with the case.86

84 Interview, April 2014.
ment warned against “propagating religious sectarianism through social media or mobile phones.”

At least one other blasphemy case based on a Facebook post was pending in a court in south Punjab at the end of the coverage period of this report.87

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.88

In 2013 the upper house of parliament passed the Fair Trial Act,90 allowing security agencies to seek a judicial warrant to monitor private communications “to neutralize and prevent [a] threat or any attempt to carry out scheduled offenses.” 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 ($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.93

ISPs, telecommunications companies, and SIM card vendors are required to authenticate the Computerized National Identity Card details of prospective customers with the National Database Registration Authority before providing service.94 As of April 2014, SIM cards in Sindh and Balochistan could only be activated through biometric verification using the customer’s fingerprint, according to a PTA media advertisement, though observers said retail stores lacked the necessary equipment. The requirement was extended to the rest of the country in summer 2014.96

---

dia-law-minister.
88  Court documents reviewed by the author.
Pakistan

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.97 A draft Prevention of Electronics Crimes Act 2014, though it contains some procedural safeguards for cybercrime investigation by law enforcement agencies, could grant intelligence agencies unrestricted mass surveillance powers.98 Critics said it lacked clear definitions, while criminalizing some specific activity like “defamation of women.” 99 Civil society groups recommended it be amended in accordance with international standards.

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.100 The analysis found FinFisher’s command and control servers in 36 countries globally, including Pakistan, on the PTCL network. This does not confirm that actors in Pakistan are knowingly taking advantage of its capabilities. Nevertheless, civil society organizations called on PTCL to investigate and disable FinFisher tools.101 Pakistan has separately been reported to be a customer of Narus, a U.S.-based firm known for designing technology that allows for deep-packet inspection of internet communications.102 Some media reports say Pakistani authorities have acquired surveillance technology from China.

Pakistan is one of the world’s most dangerous countries for traditional journalists, with five killed in relation to their work in 2013.103 Violence has yet to affect online journalists in the same way, though they can also be vulnerable. In particular, 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.104 She survived and was awarded the Nobel Peace Prize in 2014.

At least four women were killed for reasons involving technology in rural areas of Pakistan during the coverage period of this report. In June 2013, Arifa Bibi, a mother of two, was stoned to death by local men after a tribal court in the Dera Ghazi Khan region of Punjab convicted her of possessing a

98  This data includes the “communication’s origin, destination, route, time, data, size, duration or type of underlying service.”
mobile phone. The same month, a group of men fatally shot a mother and two daughters in Gilgit Baltistan, a far-northern region bordering Afghanistan. A video of the women playing in the rain had been circulating on local mobile networks. News reports said family members of the victims were involved in carrying out both incidents.

In April 2014, a man confessed to killing three men he had identified as gay via interactions on social media. Homosexuality is illegal in Pakistan, so digital communication arguably facilitated his selection of targets.

Militant Islamic groups have launched attacks on cybercafes and mobile phone stores in the past for encouraging moral degradation. None were documented during the coverage period of this report.

Free expression activists and bloggers have also reported receiving death threats. Many publicize them—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. Human rights activist Sabeen Mehmood received death threats in 2013 after opposing an anti-Valentine's day campaign by a religious group earlier in the year.

Technical attacks against the websites of nongovernmental organizations, opposition groups, and activists are common in Pakistan but typically go unreported due to self-censorship. Minority organizations such as the Catholic-run human rights advocacy group National Commission for Justice and Peace have also been subject to technical attacks. The websites of government agencies are also commonly attacked, often by ideological hackers attempting to make a political statement. In one example, an unidentified hacker defaced the electoral commission's website in advance of elections.

---


Philippines

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>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>25</td>
<td>27</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Key Developments: May 2013 – May 2014

- In February 2014, the Supreme Court upheld a contested provision in the Cybercrime Prevention Act of 2012 punishing online libel with jail terms up to eight years (see Violations of User Rights).

- The Supreme Court struck down other Cybercrime Prevention Act provisions that would have allowed warrantless content blocking and real-time monitoring (see Limits on Content and Violations of User Rights).

- The Magna Carta for Philippine Internet Freedom was filed in the Senate to repeal the Cybercrime Prevention Act (see Limits on Content).

- The Philippine National Police stepped up anti-cybercrime operations even while the cybercrime law was suspended (see Violations of User Rights).
Introduction

Freedom of expression online took a contentious turn in the Philippines after the Supreme Court finally ruled on the Cybercrime Prevention Act of 2012 a year after suspending the law to examine its constitutionality. On February 11, 2014, the court struck down provisions from the act which would have allowed content restrictions and warrantless monitoring of internet traffic by law enforcement in real time. However, it upheld the most contested provision, punishing online libel with up to eight years’ imprisonment.1 In the meantime, the anti-cybercrime unit of the national police—a group formed based on Section 10 of the law—stepped up operations in spite of its suspension.

During the coverage period of this report, Senator Miriam Defensor Santiago filed the Magna Carta for Philippine Internet Freedom seeking to repeal the cybercrime law. The bill, if passed, would significantly improve safeguards for freedom of expression online. It is also the first in the Philippines to be written incorporating direct input from internet users. Democracy.Net.Ph, an online group advocating freedom of expression, headed this initiative to make citizen input via ICTs a fundamental part of the legislative process.

Mobile phone use is widespread in the Philippines, but has yet to significantly boost internet penetration which remains comparatively expensive, in part because two major telecommunication companies have swallowed up lesser players through mergers and acquisitions. Inadequate information and communications technology (ICT) infrastructure has also slowed down penetration, and state-level efforts aim to address a longstanding digital divide between urban and rural areas.

Obstacles to Access

Internet penetration in the Philippines stood at 37 percent in 2013.2 Usage is concentrated in urban areas, with rural areas largely underserved.3 However, most users still rely on dial-up connections; just 2.6 percent of the population had fixed broadband in 2013.4 Mobile phone subscriptions, on the other hand, have increased significantly in recent years, with penetration reaching 107 percent in 2013, indicating that some users have more than one device.5 Mobile internet lags behind. One source put smartphone penetration at just 15 percent in 2013.6

5 International Telecommunication Union, “Mobile-Cellular Telephone Subscriptions, 2000-2013.”
6 Upgrade, “PH’s Smartphone Penetration Rate Lowest in Asia Pacific; Tablet Ownership Also Low,” http://www.upgrademag.com/web/phs-smartphone-penetration-rate-lowest-in-asia-pacific-tablet-ownership-also-low/.
another documented mobile broadband subscriptions at 4 percent of the population.\(^7\) Despite this, rivals Globe Telecommunications and Philippine Long Distance Telephone (PLDT) wireless subsidiary Smart Communications introduced devices for faster 4G LTE and HSPA+ data networks in late 2013,\(^8\) with the latter claiming a capacity to cover 85 percent of the population.\(^9\)

The government does not place any known restrictions on internet connectivity. Indeed, bridging the digital divide through development of ICT infrastructure is one of the goals of the government’s Philippine Digital Strategy for 2011 to 2016. Together with the United States Agency for International Development and Microsoft Philippines, the ICT Office of the Department of Science and Technology launched “Super Wi-Fi” connectivity in mid-2013 in Visayas.\(^10\) It uses TV White Space technologies—which tap previously unused frequencies and overcome physical obstacles—to increase connectivity in poor rural areas.\(^11\) However, steep broadband subscription fees still stand in the way of higher penetration in a country where 42 percent of the population lives on US$2 a day.\(^12\) In December 2013, the multistakeholder coalition Alliance for Affordable Internet reported that lower income households would have to spend nearly 40 percent of their income to afford fixed broadband access, or 20 percent for mobile broadband.\(^13\) Even as legislators urged telecoms to cut rates by 50 percent in order to promote universal access,\(^14\) the minimum monthly subscription fee for fixed broadband slightly increased from last year, when it was less than $20. In early 2014, PLDT charged $22, while Globe charged $24 for a maximum speed of 2 to 3 Mbps.\(^15\)

An industry monopoly has contributed to these inflated costs. In the 1990s, government legislation allowed competitors a foothold in the 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.\(^16\) 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,\(^17\) and was still planning to acquire provincial companies, according to late-2013 news reports.\(^18\)


\(^15\) Rates published by PLDT and Globe Telecom, February 2014.


Although the industry appears to have diversified, some of these changes are superficial. The government reported 320 registered internet service providers (ISPs) as of 2011.\(^{19}\) Yet most connect through the 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,\(^{20}\) the company now owns or partly owns five out of nine international cable landings.\(^{21}\)

Globe Telecommunications became the sole challenger to PLDT after it purchased debts from struggling competitor Bayan Telecommunications in early 2013.\(^{22}\) The rivalry has not resulted in the kind of competition which reduces costs and increases efficiency for the end user. After being mired in negotiations over interconnecting their networks for several years and delaying the development of broadband services in many areas, PLDT and Globe finally arrived at an interconnection agreement in focal parts of the country, but so far, only for landlines.\(^{23}\) Interconnection allows customers to communicate with rival networks without incurring extra costs.

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, which 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. 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.

Institutions governing the ICT sector are highly bureaucratic, often with ambiguous or overlapping responsibilities which slow the pace of development. Successive government administrations have modified the structure of official ICT bodies, including President Benigno Aquino. His Executive Order 47 of 2011 established an Information and Communications Technology Office under the Department of Science and Technology (DOST) tasked with conducting research, development, and capacity-building in the ICT industry.\(^{24}\) 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, was hard to perceive.

A streamlining process is anticipated. In 2012, Senate Bill No. 50 created a specialized Department of Information and Communications Technology. Since March 7, 2012, the bill remains pending before


a bicameral conference committee before being transmitted to the president for approval.\textsuperscript{25} If approved, all other ICT-related agencies will be abolished and their powers and personnel transferred to the new department.

All relevant government bodies are headed by presidential appointees. Critics believe this creates a dependence on the incumbent administration, which determines their budget.\textsuperscript{26}

**Limits on Content**

In February 2014, the Supreme Court struck down provisions of the 2012 Cybercrime Prevention Act which would have enabled the justice department to “restrict or block” a range of online content without a court order.\textsuperscript{27} There are no signs it was implemented during the coverage period while the law was on hold, despite some internet users’ fears it had been evoked to block a torrent site allegedly hosting pirated entertainment content.

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 of this report. Social networks and communication apps including YouTube, Facebook, Twitter, and international blog-hosting services, are freely accessible.

Section 19, the infamous “takedown” clause of the Cybercrime Prevention Act that was signed into law on September 12, 2012, would have allowed the Department of Justice to “restrict or block” content without a court order, including some overly broad categories like “cybersex,” which failed to differentiate between consensual and illegal acts.\textsuperscript{28} The Supreme Court issued an indefinite restraining order on the law in 2013 to consider its constitutionality. In early 2014, the court postponed its ruling after voting among the justices became “complicated.”\textsuperscript{29} In February, however, the Supreme Court ruled the section unconstitutional, while upholding other provisions criminalizing online libel (see Violations of User Rights).

In June 2013, the Intellectual Property Office (IPO) blocked the torrent hosting website kat.ph as an antipiracy measure under administrative powers it was granted in 2011. Some observers mistakenly feared the IPO was invoking the “takedown” clause as a proxy for the Department of Justice.\textsuperscript{30}

---


\textsuperscript{26} Erwin A. Alampay, “ICT Sector Performance Review for Philippines.”


Philippines

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."34

There have been no reports of officials putting pressure on online journalists or bloggers to delete content that is critical of the authorities. However, 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 online output, the degree is difficult to establish. Notably, however, one of the Senate’s main proponents of the libel clause in the Cybercrime Prevention Act argued that it would instill self-censorship in internet users—the actual phrase was “think before you click,” according to local blogger Raissa Robles.

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. In 2011, the Department of Education negotiated with the Department of Budget Management to increase funding for state universities and colleges for fiscal year 2012 after a “planking” protest, where demonstrators lay face down in the street, was organized via online petition against projected budget cuts. In 2013, internet users mobilized to protest the alleged misuse of PHP 10 billion ($220 million) from a Priority Development Assistance Fund locally dubbed the “pork barrel,” by senators and congressmen. A Facebook petition called for the abolition of the fund and the filing of criminal charges against the lawmakers. Nationwide protests dubbed the Million People March on August 26, incidentally the country’s National Heroes Day, and attended by 350,000 protesters in Manila alone. Following the protests, the Supreme Court declared the fund unconstitutional on Novem-

On April 1 the following year, the Office of the Ombudsman announced that it found probable cause to indict three senators and several NGO officials for plunder.41

**Violations of User Rights**

In February 2014, the Supreme Court upheld the contentious libel provision in the Cybercrime Prevention Act, maintaining criminal penalties of up to eight years’ imprisonment for online libel—double the maximum sentence for regular libel under the penal code. However, it clarified that commenting on a libelous post would not be penalized, and struck down other sections which would have allowed authorities to access computer data without a warrant. In the meantime, a police anti-cybercrime unit formed under the law continued to operate, ignoring its suspension in 2013. Besides the Magna Carta for Internet Freedom, two other positive bills made progress towards passage, including an act that would allow citizens to comment on pending bills via ICTs and a freedom of information bill that has been pending for the past 22 years.

The Bill of Rights of the 1987 constitution protects freedom of expression (Section 4) and privacy of communication (Section 1).42 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.43

Section 4c (4) of the 2012 cybercrime law, however, classified libel as a cybercrime. Section 6 stipulates a higher degree of punishment and fines for the identical offense perpetrated offline, which is punishable by six months’ to four years and two months’ imprisonment under the revised penal code.44 The Supreme Court suspended implementation of the law after widespread protests, but in a long-awaited decision handed down in February 2014, 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 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.45 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

43 Department of Justice, Resolution No. 05-1-11895 on Malayan Insurance vs. Philip Piccio, et al., June 20, 2007. Article 353 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.
28 that gives the department 90 days to produce the IRR.\(^4^6\) After seven public consultations, with the final session held on May 16, the justice department has yet to release the final document.\(^4^7\)

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 criminalized under the bill.\(^4^8\) It would further mandate the dissemination of public information as long as such information does not go against provisions in existing laws.\(^4^9\)

The Magna Carta initiative was supported by Senator Teofisto Guingona III, who filed the Crowdsourcing Act of 2013 in July. 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: the people’s committee hearings shall be held in Congress (Section 6); continuous online participation by the people while debates are being held on the floor (Section 7); and a pre-approval consultation (Section 8) wherein the President of the Philippines, before signing a bill into law, must allow people to send online comments about the bill for five days and subsequently consider the comments for at least another three days.\(^5^0\) Both bills are still pending in the Science and Technology Committee a year after they were filed.

In another welcome development, the Senate approved the People’s Freedom of Information Act of 2013 on its third and final reading on March 10, 2014, 22 years after it was first filed in Congress.\(^5^1\) Its counterpart in the lower chamber is still awaiting concurrence. It is not clear how long it would take legislators to pass it into law, though the speaker of the house promised to approve it before the end of 2016.\(^5^2\) Like the Crowdsourcing Act and the Magna Carta for Internet Freedom, this would also require the government to provide information to the people upon request, subject to national security or data privacy exceptions.\(^5^3\) Overlapping provisions from the three bills could yet be combined.

Despite the Supreme Court’s positive ruling to block the cybercrime law’s potential for abuse of privacy, some fear that Philippine authorities have already used it as a basis to conduct unauthorized surveillance. Acting on Section 10 of the law, the Philippine National Police created an anti-cybercrime group in March 2013,\(^5^4\) said that the restraining order on the law was hindering their opera-


tions, and warned that they would pursue violators in spite of it. While most publicized investigations involved online fraud or child pornography, some internet users feared legitimate activity like online dating might also be targeted under the law’s overbroad parameters. Media reports did not provide details of the surveillance and monitoring methods the group used to gather evidence. In February, the group said cybercrime investigations were ongoing in 31 out of a total 81 Philippine provinces. The first case filed under the act following the Supreme Court’s decision involved unauthorized financial transactions.

A 2012 Data Privacy Act established parameters for the collection of personal financial information and an independent privacy regulator. 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,” though it does require them to “obtain” and “preserve” evidence of violations, and threatens to revoke their license for non-compliance; 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 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 users register to subscribe to internet and mobile phone services, 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 officials and law enforcers to call on Congress to pass a law requiring the registration of SIM cards for prepaid subscribers.64

Violence against journalists is a significant problem in the Philippines. As of April 2014, the Committee to Protect Journalists reported at least 76 Philippine journalists had been killed in relation to their work—most covering political beats—since the organization started compiling records in 1992.65 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. There have been no prominent cases reported of attacks on bloggers for online expression, though some fear that may change as internet penetration grows and more people turn to web-based news sources.

There have been no reports of politically motivated incidents of technical violence or cyberattacks perpetrated by the government towards private individuals. The hacktivist group Anonymous Philippines claimed responsibility for defacing several government and private websites in November 2013 at the height of the protests against the cybercrime law and the pork barrel scam.66 On November 5, police detained and questioned five self-identified members of the group during an anticorruption rally outside the House of Representatives; they were released without charge.67 A week later, the National Bureau of Investigation traced an IP address they said they had links to illegal hacking to an internet shop in the southern Philippines, where they arrested one customer; the bureau said he could face charges.68

## Russia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partly Free</td>
<td></td>
<td></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>19</td>
<td>22</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>54</td>
<td>60</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

| Population:                             | 143.5 million |
| Internet Penetration 2013:              | 61 percent   |
| Social Media/ICT Apps Blocked:          | No            |
| Political/Social Content Blocked:       | Yes           |
| Bloggers/ICT Users Arrested:            | Yes           |
| Press Freedom 2014 Status:              | Not Free      |

### Key Developments: May 2013 – May 2014

- On December 30, 2013, President Vladimir Putin signed a bill granting the Prosecutor General the authority to place websites on the federal blacklist if the sites contained extremist content or calls for participation in unsanctioned public actions. The law was subsequently used to block access to independent media or opposition websites reporting on the unfolding conflict in Ukraine (see Limits on Content).

- Evidence of increased government surveillance of ICTs emerged in the run-up to the 2014 Sochi Winter Olympic Games (see Violations of User Rights).

- In May 2014, the government passed a law requiring certain online bloggers or social media users to register with the telecommunications regulator, which effectively limited citizens' ability to anonymously publish ideas and information online (see Violations of User Rights).

- Online journalists and bloggers continued to face legal harassment and threats of physical violence. In July 2013, a correspondent for the online media outlet Caucasian Knot who had been reporting in Dagestan was murdered, after facing repeated threats (see Violations of User Rights).
Introduction

Russia’s environment for internet freedom declined significantly as the government took multiple steps to increase control over the online sphere, particularly in advance of the Sochi Olympic Games in February 2014 and throughout the ongoing crises in Crimea and eastern Ukraine.

At the end of 2013, Putin signed a law allowing for the Prosecutor General’s office to direct the telecommunications authority to block websites that contain extremist content or calls for participation in unsanctioned public actions. The law was subsequently used to block access to independent media sites reporting on the unfolding conflict in Ukraine. Additionally, the State Duma passed amendments to the copyright legislation of the Russian Civil Code that allow for new measures to block websites that are suspected of hosting copyright-infringing material before court proceedings take place. In May 2014, the State Duma also passed a law requiring bloggers or social media users with more than 3,000 daily views to register with the government or face the possibility of having their account blocked.

Independent media outlets that were critical of the Kremlin faced increasing obstacles including economic constraints and pressure on their executive staff. Lenta.ru, one of the oldest and most widely read Russian online media sites, received a warning from Roskomnadzor on March 11 for their coverage of the crisis in Ukraine; the next day, the editor-in-chief was fired. In February, the independent TV channel Dozhd came under attack under false pretexts, leading to the majority of networks and internet TV channels to cancel their broadcasts of the station’s programming. Having lost the majority of its advertising revenue, the channel was on the brink of collapse and continues to operate almost entirely on crowdfunded donations.

Internet users in Russia faced increasing prosecutions, physical violence, and evidence of growing surveillance over the past year. According to a report published in February 2014 by eLiberator.ru, a project supported by the AGORA Association, there were 24 episodes of violence against bloggers and online journalists in 2013, including the murder of a correspondent for the online news outlet Caucasian Knot in July. In November 2013 a well-known blogger who had reported on local corruption was charged with bribery, insulting an official, and misleading the authorities, and was sentenced to 18 months in a labor camp. Surveillance of online communications without sufficient judicial oversight continues (court orders are technically required but ISPs cannot request to see the court order), and evidence of increased surveillance emerged over the past year.

Obstacles to Access

The internet penetration rate in Russia continued to grow over the past year, though not as rapidly as in previous years. According to the International Telecommunication Union (ITU), the internet penetration rate reached 61 percent by the end of 2013, compared to 53 percent in 2012 and just 27 percent in 2008.1 According to the Public Opinion Foundation, the number of people 18 years or older who access the internet on a monthly basis reached 66.5 million, or 57 percent of the

---

population, by the end of 2013, while the daily audience of internet users is estimated at about 53.2 million, or 46 percent.\(^2\)

Additionally, internet access has become less expensive and speeds have increased over the past year. According to a Yandex report, the speed of broadband internet access has significantly increased, while costs have reduced fourfold. A connection speed of 1 Mbps costs an average of US$0.72 per month, while the residents of Moscow, for instance, pay US$14 per month for access speeds averaging 51 Mbps.\(^3\)

The mobile phone penetration rate reached 168 percent, or approximately 240 million subscribers, by the third quarter of 2013.\(^4\) According to another report by the research company TNS Russia, approximately 50 percent of internet users access the internet via mobile devices.\(^5\)

The past year witnessed the massive implementation of LTE standard in Russia and access to 4G networks was available in nearly all regional centers. Mobile operators have started to offer economy tariffs for mobile service, allowing users access to the 4G/LTE network for approximately US$5.50 per month.\(^6\)

In March 2014, new amendments to the law on communications came into effect that established general requirements for providing universal communication services to citizens. According to the amended law, at least one point of collective access to telephone communication services must be installed in every settlement in the country in order to provide free access to emergency services. Settlements with a population of over 250 people must be equipped with at least one access point to the internet, which should provide the ability to transfer data at speeds of more than 10 Mbps.\(^7\) However, according to an official government report, approximately 8 percent of settlements with a population of less than 10,000 (1,343 townships) still have no access to cellular networks or the internet.\(^8\)

The market for broadband internet access remains highly concentrated in the hands of a few companies. According to the most current data available, the six largest providers occupy 77.1 percent of the market: the state-owned provider Rostelecom controls 38.6 percent of the market, while the rest is divided among ER-Telecom, VimpleCom, MTS, Trantelecom and AKADO.\(^9\) The mobile communications market is even less diverse, with the four biggest operators—MTS, Megafon, VimpleCom and Tele2—together controlling 92 percent of the market.

---


\(^3\) Internet in Russian regions, http://company.yandex.ru/researches/reports/2013/va_internet_regions_2013.xm [In Russian]


\(^9\) Advanced Communication & Media, “Cellular Data”, accessed March 12, 2014
On July 17, 2013 the Ministry of Communications published a concept paper titled, “Theses for the concept of development of multi-service networks for public communication in the Russian Federation,” which would centralize the management of trans-boundary internet traffic. The proposal would grant the right to transmit foreign internet traffic to only a few federal service providers, effectively forcing all other ISPs to buy the traffic from them. The requirements of the federal service provider are so strict that currently only a single state-owned company, Rostelecom, would be able to meet them. If the proposal is approved, it is likely that Rostelecom will control an even greater share of the market.

The ICT and media sector is regulated by the Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications (Roskomnadzor) under the control of the Ministry of Communications and Mass Media and the Government of the Russian Federation. The head of Roskomnadzor, Alexander Zharov, was appointed directly by executive decree on May 3, 2012. The regulatory body has the authority to determine if a website should be blocked based on whether or not the site contains material that is restricted by the law; these decisions do not require prior court approval. Additionally, 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 (see Limits on Content). As a result, Roskomnadzor has become a primary player in the field of controlling and filtering information on the internet.

Limits on Content

From 2013-2014, the Russian authorities significantly expanded restrictions on online content through the introduction of additional legal grounds for blocking access to websites. On December 30, 2013, Putin signed a bill granting greater authority to the Prosecutor General to block websites without a court order if the websites allegedly contained extremist material or calls for participation in unsanctioned public actions. Up until the end of 2013, the practice of blocking online content in Russia was relatively untargeted—many individual websites or webpages were blocked for containing “harmful” or “extremist” content, but independent news outlets were still largely able to operate online. Indeed, the internet was regarded as a space for freedom of expression and freedom of information that was distinctly separate from—and largely immune to—the firm state control over the print and broadcast media. After this law came into effect on February 1, 2014, however, it was quickly used to crack down on online media outlets with content critical of the Kremlin’s policies, particularly regarding the conflict in eastern Ukraine and Crimea.

On March 13, 2014, just three days before 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 the Bolotnaya protestors in 2012; Ezhednevny Zhurnal (Ej.ru), a news and opinion site; and Kasparov.ru, the website of former chess champion turned opposition figure, Gary Kasparov. The owners of the websites were not provided with an explanation as to what content had violated the law and caused the Prosecutor General to issue the blocking order. At the same time, the authorities blocked access

---

10 ICT Ministry official website. [In Russian]
11 Access to a number of online resources calls for unauthorized mass events was blocked. Roskomnadzor official website, March 13, 2014, [In Russian]
to the personal blog of the opposition leader Alexei Navalny and the website of the radio station Echo of Moscow (Ekho Moskvy), though these two were subsequently unblocked within a few days.12

In the first half of 2014, Roskomnadzor reported blocking 85 websites for containing “extremist content,” based on orders from the Prosecutor Generals’ office.13 In addition to the new amendments passed in December 2013, websites can still be blocked in accordance with Federal Law 139-FZ if they are placed on the Unified Register of banned sites, operated by Roskomnadzor, for containing illegal or otherwise harmful material such as child pornography, material related to drug abuse, and so forth. According to the official report of Roskomnadzor published on December 13, 2013, the Unified Register contains 3,361 records, including 894 IP addresses. Experts at the RosComSvoboda project claim that this has led to the blocking of more than 50,000 sites in Russia.14

On July 17, 2013, the State Duma passed amendments to the copyright legislation of the Russian Civil Code, allowing for new measures to block websites that are suspected of hosting copyright-infringing material. The law allows for the court to grant preliminary injunctions in cases of alleged copyright infringement online, in which case the person responsible for the website where the content is hosted has 24 hours to remove the content after notification, otherwise the website host company will be instructed to restrict access to that website. However, once the court issues the preliminary injunction, the website is blocked while the court waits for the applicant to file the official complaint, potentially before the website owner is even notified of the case.

Russian legislation contains a wide range of prohibited information, including images that offend religious feelings, or content related to suicide or illegal drugs. Thus, in most cases there are no clear criteria for evaluating information, and public authorities, when considering the decision to block content, do not always offer clear rationale for such a restriction. The lack of clear legislation for blocking banned content leads telecom operators, in some cases, to carry out the widest blocking possible so as to avoid fines and or having their license revoked. During 2013, Russian courts issued 429 decisions on the administrative liability of telecom operators for failing to block prohibited information.15 For example, in September 2013, Roskomnadzor sued at least three ISPs for 30,000 rubles (approximately US$900) for failing to log in to the register of banned websites. Presumably the ISPs could not be following the blocking orders if they had not checked the list of banned websites, and would therefore be in violation of the law, although the proceedings did not specify whether the ISPs were found to have actually provided access to any of the sites on the list.16

Online media outlets also suffer as a result of ISPs’ decisions to block access to more than the prohibited content. For instance, Rostelecom, referring to the technical inability to block single pages in mid June 2013, denied access to the entire websites of Gazeta.ru and Komsomolskaya Pravda in the Ulyanovsk Region, after the Leninsky court ruled that content about bribery of officials that was

---

previously featured on the websites “undermined the authority of the government.”\textsuperscript{17} Access to the sites was restored on June 26 after the prosecutor clarified the blocking order.\textsuperscript{18}

Self-censorship among average internet users is not a pervasive trend in Russia, aside from categories of speech that are prohibited by law. However, bloggers and editors of online media outlets have faced increasing government pressure over the past year, which may have had a chilling effect on online freedom of expression more broadly. Additionally, recent government efforts to restrict anonymous communication online may also have an impact on what internet users feel comfortable expressing online (see Violations of User Rights).

Over the past year a number of independent media outlets found themselves under the threat of closure or were forced to change their editorial policy. On March 11, 2014, one of the oldest and most widely read Russian online media sites, Lenta.ru, received a warning from Roskomnadzor in connection with the publication of an interview with one of the leaders of the Ukrainian movement “Pravy Sector” (“The Right Sector”), who took an active part in the confrontation with Berkut forces during the Euromaidan protests in Kyiv. The next day, prominent businessman Alexandr Mamut, who controls part of the media company that owns Lenta.ru, dismissed editor-in-chief Galina Timchenko without explanation and replaced her with a government relations specialist, Alexey Goreslavskay. It is unlikely that the dismissal of the editor could be explained by financial motives, as Lenta.ru, with 20 million unique visitors in February,\textsuperscript{19} was bringing in 15 to 20 percent of the total profit for media holding company Afisha-Rambler-SUP.\textsuperscript{20} In response to the dismissal, 77 correspondents and members of the editorial staff posted an open letter on the website stating that the dismissal of Timchenko amounted to government censorship and a violation of the law on mass media. Thirty-nine of these staff members additionally resigned in protest.

VKontakte, Russia’s leading online social network, has also reportedly come under increasing pressure from the government over the past year. Beginning in December 2013, Pavel Durov, the founder and CEO of VKontakte, reported that the Federal Security Service (FSB) had sent him requests to hand over the private data related to the accounts of several Euromaidan activists. Durov refused to comply with this request. Previously, the FSB had issued orders for VKontakte to block the pages associated with Alexei Navalny, the anti-corruption and opposition figure. In April, Durov announced that he was resigning due to this ongoing pressure and was leaving the country. In September 2014, the email provider Mail.ru, owned by Kremlin-friendly businessman Alisher Usmanov, officially took control over VKontakte.

Other forms of pressure on internet outlets have also been used in the past year, as Roskomnadzor continued to issue warnings to the media. At least four editorial boards (for the websites Grani.ru, Obeschaniya.ru, Sibkray.ru, and Polit.ru) received warnings from the court in Novosibirsk in June 2013 for publishing one of the banned icons associated with the punk-protest group Pussy Riot. Other websites, including Neva24.ru, KM.ru, the information agency “Novyi Region,” and Regions.

\textsuperscript{17} Gazeta.ru has been blocked in Ul’yanovsk, Gazeta.ru, June 25, 2013, \url{http://www.gazeta.ru/social/2013/06/24/5391777.shtml} [In Russian]

\textsuperscript{18} Index on Censorship, “Russia: We know what you blocked this summer,” October 1, 2013, \url{http://www.indexoncensorship.org/2013/10/russia-censored-summer-2013/}

\textsuperscript{19} Sultan Suleimanov. Retro: That’s all. TJournal.ru. March 14. 2014 [In Russian]

ru — also received warnings for publishing links to video of punk-prayer by Pussy Riot. Given that media outlets can be forced to close if they receive two court warnings within a 12 month period, most of the outlets chose to remove the images.

Russian authorities continue to use the assistance of paid commentators to influence online content. An investigation conducted by journalists at Novaya Gazeta showed that some members from the pro-Kremlin youth movements “Nashi” and “Molodaya Gvardiya” organized paid campaigns in social networks. In January 2014, the editors of the German newspaper Die Zeit reported a wavelike increase in the number of anti-Western comments, believed to be propaganda, on the paper’s website at the time of the Euromaidan protests in Ukraine. Other media outlets, including Forbes and the Guardian, reported similar flooding of “insulting, combative” comments on any articles posted online related to Russia or Ukraine.

Pressure from the government has also made it more difficult for independent media outlets to maintain their economic viability. The independent media outlet Dozhd TV, which also broadcasts online, does not receive government funding and exists solely on advertising revenue. The editorial policy of the channel is very different from state-controlled television; for example, Dozhd TV was the only Russian TV channel that broadcasted live from Kyiv during the early stages of the Euromaidan protests. Beginning in early 2014, Dozhd TV came under fire from the government after it aired a debate in January asking whether Leningrad should have surrendered during the 900-day-long siege in World War II. Within a month, the majority of the largest satellite broadcasting operators and cable networks, and internet TV providers such as NTV-plus, AKADO, Dom.ru, Rostelecom and TricolorTV, simultaneously refused to broadcast the channel, in what some attributed to a coordinated government crackdown on independent media. Dozhd reportedly lost nearly 90 percent of its audience, leading to a catastrophic reduction in advertising revenue—some companies reportedly left because of the loss in viewership, others because of direct government pressure. Additionally, in March 2014, the company that owns the building where Dozhd operates announced that it was refusing to renew Dozhd’s lease for the following year, forcing the media outlet to relocate. Faced with these developments, Dozhd was on the verge of collapse and has had to ask for financial support from viewers. Currently, Dozhd continues to function due to the success of these crowdfunding efforts.

Despite government pressure against independent media outlets, the online sphere in Russia remains relatively diverse, particularly content on blogs or forums. Social networks like VKontakte, LiveJournal, and Facebook continue to be a significant tool for mobilization and communication between citizens and activists. In 2011, opposition activists in Moscow used Facebook to organize street protests in reaction to the December 2011 State Duma elections, although local platforms like Vkontakte are more popular tools for political mobilization in other regions. Organizers of subsequent protests, such as those related to Putin’s inauguration in May 2012 and the January 2013 “March Against Scoundrels” protesting the bill banning American’s adoption of Russian children, have

---

22 Annika von Taube, “Russische Botschaft,” Zeit Online, January 27, 2014, [In Russian]
23 Tikhon Dzyadko, “Triumph of the will: Putin’s war against Russia’s last independent TV channel,” The Guardian, April 10, 2014, [In Russian]
also made use of social networking platforms to call attention to events. Additionally, crowdfunding websites such as RosUznik.org, which raises money for and coordinates the legal defenses of civil activists charged in the Bolotnaya Case, have emerged as a way for opposition activists to organize support efforts online.25

Violations of User Rights

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, during 2013 and early 2014, Russia adopted a complex set of laws and other acts, which, coupled with repressive law enforcement and judicial practices, have reduced the constitutional guarantees of freedom of speech. Additionally, surveillance and detentions of online activists have increased. Courts tend to side with public authorities, refusing to apply directly applicable provisions of the constitution and international treaties of the Russian Federation.

In July 2012, the State Duma passed amendments to the criminal code that recriminalized defamation, after having just decriminalized it less than a year earlier. Revisions to Article 129 of the code officially make defamation a criminal offense, with penalties including a fine of up to RUB 5 million (approximately US$138,000). Over the past year there were more criminal charges for illegal activity on the internet, and punishments for posting extremist content (which often refers to criticism of the authorities) were also increased.

During 2013 there were more than 200 cases of criminal prosecution against internet users for the dissemination of information online.26 The majority of these criminal cases were connected to right-wing publications on social networks. The usual penalty for these crimes is correctional work, probation or fines. In addition to these cases, however, there were also prosecutions launched against politicians, activists, and journalists. One of the more troubling cases of politically-motivated prosecution involved Sergei Reznik, a well-known blogger who reported on alleged corruption involving local officials. In November 2013, a court sentenced Reznik to 18 months in a labor camp on charges of bribery, insulting an official, and misleading the authorities.27

In March 2013, Mikhail Afanasyev, the editor-in-chief of the online media outlet Novy Fokus, was charged with criminal defamation for publishing an opinion piece online in which he accused a police officer of lying about him in court. Previously, Afanasyev had been arrested on charges of hooliganism for attempting to video record an arrest, though these charges were later dropped. On September 6, 2013, Afanasyev was acquitted of the criminal defamation charges.

Opposition leader and prominent blogger Alexei Navalny has faced prosecution multiple times over the past few years. On April 22, 2014, Navalny was found guilty of libeling a district councilor on Twitter and was fined US$8,400. Under house arrest at the time of the alleged Twitter post, Navalny denied posting the tweet, as his house arrest precluded him from using the internet. His spokesperson stated that the case was politically motivated and was intended to move Navalny from house arrest to pretrial detention.28

Privacy and anonymity are key concerns for many online users in Russia. On May 5, 2014, Putin signed a law that considers any website with over 3,000 viewers, including blogs and social media accounts, to be “mass media.”29 The law requires these outlets to register with the government, thus decreasing the space for these users to communicate anonymously online. Additionally, the new measure contained wording that would require any services hosting such platforms to maintain records of these users’ data on servers located within Russia, a provision which was further substantiated by a broader data localization law passed in July 2014 that requires all foreign internet companies to host Russians’ data on servers within the country.30

There are currently no restrictions on the use of circumvention tools or anonymizers, although 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 is developing a package of laws to block access to Tor and foreign proxy-servers for Russian users.31 Presently, identification is needed for signing a contract for internet access or cellular services. Additionally, owners of public Wi-Fi spots are required to use content filters to protect children from potentially accessing “harmful” information (Article 6.17 of the code of administrative offenses). This requirement may force owners to implement age checks for users.

In July 2013, members of the State Duma sent a request for clarification to Roskomnadzor regarding the fact that the service Google Translate allows users to open websites that are blocked in Russia. The members reported their intent to resolve this method of circumvention; however, no further steps have been taken to date.32

The electronic surveillance system in Russia, known as the “system for operational investigative measures,” or SORM, was launched in the late 1990s, and recent evidence suggests that the Russian government has significantly increased its surveillance capabilities over the past few years. Records of government procurement documents revealed the extent to which the government had expanded its domestic surveillance infrastructure, including upgrades to telephone and Wi-Fi networks, allowing the government to extensively monitor and filter all communications during the

---

30 This broader data localization law was passed outside of the coverage period for this report. See: Paul Sonne and Olga Razumovskaya, “Russia Steps Up New Law to Control Foreign Internet Companies,” Wall Street Journal, September 24, 2014, http://online.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920.
32 “Google Translate can be used to open website which is blocked in Russia,” RG.ru, July 31, 2013, http://www.rg.ru/2013/07/31/google-site-anons.html [In Russian]
Russia

Winter Olympic Games in Sochi.\(^{33}\) Such surveillance 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 Maxim 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 so-called “extremist activities,” namely antigovernment protests.

Online surveillance represents somewhat less of a threat in the major cities of Moscow and Saint 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 license 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. At the same time, experts note that there is no information about government efforts to bring to account security officers who abuse tracking methods.\(^{34}\) ISPs and mobile operators are required to provide network access to law enforcement agencies in conducting search operations, as well as provide other information requested by the prosecutor’s office, the Interior Ministry, the FSB and the Investigative Committee.

In addition to surveillance, violence against online journalists escalated over the past year. There were at least 24 cases of violence or threats documented in 2013.\(^{35}\) On July 9, 2013, Akhmednabi Akhmednabiyev, a journalist for the online news site Caucasian Knot and the deputy editor of the independent news outlet Novoye Delo, was shot outside of his house in Dagestan. Colleagues believe the murder was politically motivated, given that Akhmednabiyev frequently reported on sensitive topics such as government corruption, arbitrary detentions, and protests.\(^{36}\) Akhmednabiyev had survived a previous assassination attempt six months earlier.

There has also been an increase in the number of cyberattacks on independent media, blogs, and news portals. Websites that suffered DDoS attacks include 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 the TV channel Dozd.

According to a Kaspersky Lab report, 2013 was marked by a 20-fold increase in power of DDoS attacks in the Russian online sphere (RuNet). The most powerful attack to date was organized against the website of Novaya Gazeta and amounted to 60 Gbps, compared to the maximum attack

---


power reflected in 2012 of 2.9 Gbps. On January 31, 2014, Novaya Gazeta reported that the police investigative department in Saint Petersburg had opened a criminal investigation into the attack; this case remains the only official response to the cyber threat to independent media.

Rwanda

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Partly Free</td>
<td>18</td>
<td>19</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>48</td>
<td>50</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 11.1 million

Internet Penetration 2013: 9 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- While ICT development continued to expand access to the internet across the country, a growing number of independent online news outlets and opposition blogs were intermittently inaccessible in Rwanda (see Obstacles to Access and Limits on Content).

- News reports in early 2014 revealed that the Rwandan government may employ fake Twitter trolls to harass, discredit, and intimidate critical voices online (see Limits on Content and Violations of User Rights).

- The Law Relating to the Interception of Communications enacted in October authorized high-ranking security officials to monitor email and telephone conversations of individuals considered potential threats to “public security” (see Violations of User Rights).

- Stanley Gatera, the editor of the independent news website Umusingi, was arrested in April on trumped-up charges of attempted extortion. Upon release, he faced death threats that led him to flee the country in exile (see Violations of User Rights).

- Foreign journalists were harassed for their critical coverage of the Rwandan government, with some reports of online harassment tied to senior officials (see Violations of User Rights).
Rwanda

Introduction

In recent years, the government of Rwanda under President Paul Kagame has embarked on an 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 remains low—hampered primarily by poverty and a lack of appropriate infrastructure, especially in rural areas—access is continually expanding due to public and private investments in broadband technology across the country, while mobile internet access is increasing at an impressive rate. Meanwhile, the proliferation of ICTs has contributed to progress in the country’s governance, health, education, agriculture, and finance sectors.¹

Though ICT development has been among the top priorities for the Rwandan government, 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. In the lead-up to the 20th anniversary of the Rwandan genocide in April 2014, a few critical news websites that had previously been blocked in 2010-2011 were intermittently inaccessible in Rwanda again throughout 2013 and 2014, while a number of critical blogs were unavailable altogether. In addition, worries remained that the government’s firm restrictions on print and broadcast media—particularly on contentious content concerning the ruling party and the 1994 genocide—will cross over into the internet sphere, as occurred when the authorities blocked the online version of an independent newspaper in the lead-up to the 2010 presidential election.

Progressive amendments to the 2009 Media Law were adopted in March 2013, providing journalists with the “right to seek, receive, give and broadcast information and ideas through media;” the amendments also explicitly recognize freedom for online communications. Nonetheless, online journalists were targeted for harassment and arrest during the coverage period. In April 2014, the editor of the independent news website Umusingi, Stanley Gatera, was arrested on trumped-up charges of attempted extortion, which the journalist believed was linked to a critical interview he conducted on Al Jazeera’s “People and Power” program—posted online and broadcast on television—in March 2014. Gatera was held for six hours and received death threats following his release, leading him to flee the country altogether.

Foreign journalists were also harassed for their critical coverage of the Rwandan government, with some reports of online harassment tied to senior officials. In early 2014, a journalist for Radio France Internationale was repeatedly harassed on Twitter by a user known as @RichardGoldston, which was later revealed to be an account operated by the president’s office. The Kagame government has also been accused of targeting political dissidents living in exile for assassination. In February 2014, Andrew Muhanguzi, the brother of the exiled editor of the independent Umuvugizi news website, was reported missing. His family claims that Muhanguzi, living in exile in Uganda, was kidnapped by men in Ugandan police uniform outside their home on February 16.

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 October 2013, the Rwandan president promulgated the Law Relating to the Interception of Communications

that authorizes high-ranking security officials to monitor email and telephone conversations of individuals considered potential threats to “public security.”

Obstacles to Access

Rwanda has made major strides in expanding access to ICTs across the country, though 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 9 percent in 2013, up from 8 percent in 2012, according to estimates from the International Telecommunication Union (ITU). By contrast, official government statistics cite a penetration rate of 22 percent as of March 2014—up from less than 2 percent in 2009—though the rate includes internet subscriptions on mobile devices, which comprise over 99 percent of all internet subscriptions. Fixed-broadband access reaches only a sliver of the population, at 0.02 percent according to the ITU.

Meanwhile, mobile phone penetration is significantly higher than that for internet access, growing from 50 percent in 2012 to over 57 percent in 2013, according to the ITU, while government figures noted a penetration rate of 65 percent in March 2014. This growth has been largely a result of increasing competition between the three main mobile phone operators—MTN, TIGO, and AIRTEL—whose respective market shares are 52 percent, 33 percent, and 15 percent. 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 further 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. According to a 2013 Gallup study, the median annual per capital income in Rwanda is US$235, while median household income is

---

5 International Telecommunication Union, “Fixed (Wired)-Broadband Subscriptions, 2000-2013.”
10 Ministry of Youth and ICT, “Measuring ICT sector performance and Tracking ICT for Development (ICT4D).”
US$1,101.11 In addition, only 11 percent of Rwandans are ICT literate,12 and over 70 percent of the population speaks only Kinyarwanda, making internet content in English inaccessible to the majority of Rwandans.13 Meanwhile, only 17 percent of Rwandan households have regular access to electricity.14

In the face of such challenges, the Rwandan government has made ICT development a high priority. In September 2013, for example, free wireless hotspots were implemented across the capital city through the “Smart Kigali” project, a public-private partnership with ISPs, hotels, restaurants, and government agencies.15 In late 2013, the government contracted Korea Telecom in a deal that aims to deliver 4G LTE broadband services to 95 percent of Rwandans within three years.16 Fixed-broadband internet services are also expanding across the country, though according to May 2014 data from Akamai’s “State of the Internet” report, internet speeds are still slow, averaging 1.4 Mbps (compared to a global average of 3.9 Mbps).17 In addition, broadband adoption in Rwanda (characterized by connection speeds greater than 4 Mbps) comprised only about 6 percent of internet users, while the country’s narrowband adoption (connection speeds below 256 kbps) comprised 14 percent of internet users.18

As a result of Rwanda’s commitment to ICT development, the cost of access is slowly decreasing. As of early 2014, a 128/64 Kbps package of wireless internet cost about RWF 64,900 (US$95).19 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$2,000.20 Meanwhile, the Broadband Systems Corporation, a local service provider, charges monthly fees of about US$30 for single users and $46 for multiple users, while the cost of using the internet in a cybercafe is approximately US$0.14 (RWF 100) for 1 hour.21

The cost of internet access via mobile phones has also declined, helping fuel the exponential growth of mobile internet users. As of March 2014, mobile internet tariffs range from RWF 30 to 50 per Mb (US$0.03 to $0.08 per Mb), and the three mobile internet companies—MTN, TIGO, and AIRTEL—

offer their customers daily bundles at RWF 500, RWF 800, and RWF 500 (US$0.72, $1.15, and $0.72), respectively. In addition, MTN Rwanda offers low-cost internet-enabled mobile phones for as cheap as RWF 9,500 (US$14).

Following the country’s market liberalization policies implemented in 2001, the number of companies providing telephone and internet services increased from one—the state-run Rwandatel—to nine ISPs and three mobile phone companies in 2014, all of which are privately owned.

The Rwanda Internet Exchange (RINEX) was set up in 2009 to connect ISPs and enable the routing of local internet communications through a central exchange point without having to pass through international networks. ISPs can also opt to connect via RINEX to the international internet. The aim, ostensibly, is to make intra-Rwandan internet communications cheaper and faster, though such control over internet traffic has the potential to facilitate efforts to systematically censor or monitor domestic online communications. As of the end of 2013, only five ISPs exchange internet traffic via RINEX. According to the ITU, the level of competition for Rwanda’s international gateway is characterized as “partial.”

The Rwanda Utilities Regulatory Agency (RURA) supervises 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, though 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. Nevertheless, RURA is generally viewed as independent in its operations.

Limits on Content

A growing number of independent online news outlets and opposition blogs were intermittently
inaccessible during the coverage period. News reports revealed that the Rwandan government may
employ fake Twitter trolls to harass, discredit, and intimidate critical voices online.

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 news content of oppositional nature. In early 2014, a test conducted
by Freedom House found that a number of independent news outlets and opposition blogs were
inaccessible; however, it was uncertain whether those sites were taken down out of the owners’
own accord or due to external pressure.

Throughout the coverage period, the website of the independent newspaper Umuvugizi—which
was suspended for six months in 2010—was intermittently inaccessible. A few opposition sites
continued to be blocked on some ISPs but were available on others, including Umusingi and
Inyenyeri News, which were both first blocked in 2011. In early 2014, Leprophete, an opposition
website based in France, was accessible on the MTN Internet ISP but blocked on AIRTEL Internet.
Content from Umusingi, Umuvugizi, and Inyenyeri News could still be accessed on their respective
Facebook pages, and other news sites that were sporadically blocked could be accessed through
their associated blogs.

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. In the
past, however, the Media High Council was known to screen web content and reportedly contacted
websites to request the removal of certain information on several occasions. 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, though no takedown requests
were documented during the coverage period. Appeals on critical media issues can be made
through the Rwanda Media Commission (RMC), the new media self-regulatory body created under
the 2013 Media Law.

Social-networking sites such as YouTube, Facebook, Twitter, and international blog-hosting services
are freely available. Given the more limited space for press freedom in the traditional media sphere,
Rwandan media outlets are increasingly going online to avoid government control or suspension
as well as heavy production costs. Nonetheless, the economic environment for online news
websites remains a challenge for independent outlets, particularly in comparison to their state-run
counterparts that receive income from government advertisements and direct subsidies.

---

32 Opposition blog websites that were unavailable as of May 2014 were: http://www.iwacu1.com, http://www.musabyimana.be,
33 Reporters Without Borders, “Persecution of Independent Newspapers Extended to Online Versions,” news release, June 11,
35 Efforts to access the Leprophete website on the AIRTEL network yields the message, “The URL is not available.”
Newspaper/127730681083696.
37 “Law No. 18/2010 of 12/05/2010, Relating to Electronic Messages, Electronic Signatures and Electronic Transactions,”
Another economic constraint on local web content presented itself in July 2013, when the Rwanda Information Communication Technology Association (RICTA)—the organization that oversees the .rw domain and represents the Rwandan internet community—announced that it would begin charging an annual subscription fee for a .rw domain name, which was previously free. Subscriptions for non-citizens now cost RWF 167,000 (US$235), while Rwandans pay RWF 30,000 (US$43)—rates that are more expensive than other domains, including the .com domain managed in the United States—though RICTA hopes to reduce the price as the number of .rw domains increase. The initiative aims to improve the accessibility of domain registration services and enhance internet access in the country.39

Given the lack of an independent press in Rwanda, 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 access information.41 In a Rwanda Media Barometer report published in August 2013 by the Rwanda Governance Board—a public body—in partnership with Transparency International Rwanda, a survey of 144 media practitioners found that nearly 50 percent of respondents practiced self-censorship “due to fear of consequences.”42 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.43 During the September 2013 parliamentary elections, an international elections observer mission noted a perception among journalists that they would be targeted for critical reportage.44

Nevertheless, the spread of social media tools has empowered Rwandans to discuss issues that were formerly taboo and not open to public discussion due to fears of persecution. The expansion of internet access has also enabled the Rwandan blogosphere to evolve into a vibrant platform for expression, even though the websites and blogs of opposition activists both within and outside Rwanda are increasingly inaccessible.45 While opposition supporters living outside Rwanda—mainly in Europe, the United States, and South Africa—are responsible for most of the criticism against the government on forums, websites, and blogs, local dissenting voices are increasingly heard in online news portals such as Igihe, especially via readers’ comments. Despite the increasing number

---

41 Rwanda Media Barometer (2013), page 49.
42 Rwanda Media Barometer (2013), page 42.
of media outlets, however, observers believe that the Rwandan media landscape represents less diversity in opinions than ever before, likely due to increasing levels of self-censorship.46

Facebook and Twitter also emerged as popular platforms for online interaction, in part as a result of the increasing use of internet-enabled phones.47 In 2013, MTN Rwanda introduced an “SMS to Twitter” tool to facilitate use of the social media platform for people without easy access to the internet on computers.48 The president is an active supporter of these social networks, occasionally using the platforms to engage in discussions with users and openly respond to issues concerning the current state of governance in the country. In 2013, Kagame and his foreign affairs minister were ranked by the “Twiplomacy” study as among the top five most conversational leaders worldwide.49

Twitter also offers Rwandans a new platform for protest and engagement with the government. For example, the Ministry of Health (@RwandaMoH and @agnesbinagwaho) regularly engaged in serious discussions with citizens and journalists over poor performance in hospitals and other health services. Nevertheless, news reports in early 2014 revealed that the Rwandan government may employ fake Twitter trolls to harass, discredit, and intimidate critical voices online (see “Violations of User Rights”).50

With mobile phones more widely accessible than the internet, text messages have become another important channel for citizens to 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, which are broadcast on the radio. Most recently, citizens challenged the education ministry over the country’s quality of education. However, the ability of citizens to use digital media for organizing large-scale street protests remained limited due to broader restrictions on freedom of assembly, particularly regarding politically sensitive topics.

Violations of User Rights

Stanley Gatera, the editor of the independent news website Umusingi, was arrested in April on trumped-up charges of attempted extortion. Upon release, he faced death threats that led him to flee the country in exile. Foreign journalists were harassed for their critical coverage of the Rwandan government, with some reports of online harassment tied to senior officials. The Law Relating to the Interception of Communications enacted in October 2013 authorized high-ranking security officials to monitor email and telephone conversations of individuals considered potential threats to public security.

Article 34 of 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. In March 2013, the state adopted progressive amendments to the 2009 Media Law, 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.\(^{51}\) The new law was also applauded 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.\(^{52}\)

The passage of the Media Law also led to some fears of increasing government control over the internet,\(^{53}\) with the freedom of expression organization Article 19 criticizing the law for containing “too many provisions which pose a threat to journalists and the independence of the media, including online media.”\(^{54}\) In particular, the new law gives the minister of ICTs unlimited powers to establish the conditions for both local and foreign media companies to operate in Rwanda.

A revised Access to Information Law was promulgated in March 2013 that allows journalists to conduct investigative journalism with more official and credible sources of information.\(^{55}\) Nevertheless, the extent to which the media should have the unchecked right to free expression is often a matter of public debate in Rwanda, with some commentators suggesting that Rwanda’s media practitioners should be cautious in their speech as long as the history of genocide continues to haunt the country.\(^{56}\)

In July 2013, a data protection law was drafted with the aim of addressing the rising cybercrime risk in Rwanda. However, the draft law provides exceptions to user data protections in the unclearly defined interest of national sovereignty, national security, and public policy, which in the context of President Kagame’s authoritarian governance, may pose a threat to individuals critical of the regime.\(^{57}\)

While there are no laws that specifically restrict internet content or criminalize online expression, Rwanda’s generally restrictive legal provisions governing the traditional media could be applied to the internet. For example, the decision to ban the online version of *Umuvugizi* in 2011 was based on charges of publishing “divisive language,”\(^{58}\) a category of expression that is criminalized by the 2001

---


Law on Discrimination and Sectarianism. 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.

A vague 2008 law against “genocide ideology” similarly threatens freedom of expression both online and off, prescribing heavy prison sentences and fines for any offender “...who disseminates genocide ideology in public through documents, speeches, pictures, media or any other means.” In response to criticisms of the law’s overly broad nature, the minister of justice proposed amendments in November 2012 that aimed to make the law more definitive and easier to interpret. Passed by both the lower and upper houses in July 2013 and promulgated in October, the amended law reduces prison sentences from 25 years to a maximum of 9 years and requires proof of criminal intent behind an offending act that must be “characterized by thoughts based on ethnicity, religion, nationality or race to foment genocide [or] support genocide.” Nevertheless, the law still restricts freedom of expression by retaining the notion of “genocide ideology” as a criminal offense and by excluding a clear distinction between a private conversation and public speech.

The Rwandan judiciary is not fully independent, and many traditional journalists view the threat of imprisonment as a key constraint on their work. Meanwhile, arrests and prosecutions of online journalists have increased in recent years. In April 2014, 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. 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, leading him to flee the country altogether.

Perceptions of media freedom and freedom of expression remain grim. In the August 2013 Rwanda Media Barometer report (referenced above), the survey of 144 media practitioners found that over 30 percent of respondents had expressed that they had been prevented from their right to freedom of expression. Among those respondents, over 48 percent reported that central government officials had deprived them of their right to expression, followed by police officers (19 percent), local government officials (14 percent), private companies (14 percent), and military agents (5 percent). While the government-sponsored report presents a somewhat critical perspective of media freedom in Rwanda with respect to government abuse of freedom of expression, the report qualifies the criticism with the assertion that “the abuse of the right to freedom of expression of which the police are accused of is justified by their mission of protecting public order.”

The ability to communicate anonymously is compromised by SIM card registration requirements initiated in early 2013 to “decrease mobile phone related crimes across the country.” SIM card owners were given the deadline of July 31, 2013 to register their cards with service providers, after which point unregistered cards were disconnected. Websites hosted on the local domain also need to register with RICTA.

Until recent years, government monitoring of online communications did not appear to be widespread, though there had been instances in past years of emails, phone calls, and text messages belonging to opposition activists being produced as evidence in trials. The sophistication of the Rwandan authorities’ surveillance capabilities is unknown, but there is growing suspicion that surveillance is pervasive, particularly after recent revelations of numerous exiled Rwandan dissidents being attacked and targeted for assassination by the Kagame regime, despite their efforts to protect their identities.

Worryingly in October 2013, the Rwandan president promulgated the Law Relating to the Interception of Communications that authorizes high-ranking security officials to monitor email

70 Rwanda Media Barometer (2013), page 40.
71 Rwanda Media Barometer (2013), page 41.
72 Rwanda Media Barometer (2013), page 42.
75 This was the case in the trial of opposition leader, Victoire Ingabire, during which e-mails and proof of money transfer to FDLR (French acronym for the Democratic Forces for the Liberation of Rwanda) rebels were used as evidence. These were mostly obtained via low-tech methods of confiscating suspects’ mobile phones and computers rather than via service providers. See: Didas Gasana and Ann Garrison, “Ingabire trial: Rwanda prosecution fails ‘evidence test,’” Rwandinfo ENG (blog), accessed February 10, 2012, http://rwandinfo.com/eng/ingabire-trial-rwanda-prosecution-fails-evidence-test/.
and telephone conversations of individuals considered potential threats to “public security.”\(^{77}\) Under the new law, communications service providers are required to ensure that their systems have the technical capability to intercept communications upon demand. According to a report from Privacy International, such interception technology may include the use of keyword scanning to identify certain topics of discussion.\(^{78}\) While the law requires government officials to apply for an interception warrant, it also includes a provision that allows for a warrant to be issued verbally in urgent security matters, to be followed by a written warrant within 24 hours.\(^{79}\)

Meanwhile, the government has been known to monitor and analyze all media content during the country’s annual genocide mourning period every April with the aim of “highlighting the civic contribution of the media during the commemoration period and discerning the extent to which media abide by legal and professional standards while covering genocide related issues.”\(^{80}\) The monitoring of online media was incorporated for the first time during Rwanda’s 18th commemoration period in April 2012, which has led to a growing sense that the authorities may be monitoring other online communications as well. The extent of the government’s media monitoring activities during the 20 year commemoration of the genocide in April 2014 is unclear.

Journalists within the country frequently face violence and harassment when attempting to cover news stories, leading some to flee the country and report in exile.\(^{81}\) According to the Committee to Protect Journalists, Rwanda ranks among the top 10 countries from which journalists seek exile.\(^{82}\) Online journalists and ordinary users, however, have not yet experienced the same level of intimidation as traditional media journalists to date, though instances of harassment and violence against online journalists increased in the past year.

In early 2014, Sonia Rolley, a journalist for Radio France Internationale, was repeatedly harassed on Twitter by a user known as @RichardGoldston.\(^{83}\) 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.”\(^{84}\) Another foreign correspondent, Steve Terrill, who

---


\(^{84}\) Twitter post by “Presidency | Rwanda” @UrugwiroVillage, March 8, 2013, 2:26 AM, https://twitter.com/UrugwiroVillage/statuses/442184647863443456.
used Twitter to publicly call on @RichardGoldston to end the harassment, was subsequently barred from entering Kigali on March 15 to cover the 20th anniversary of the Rwandan genocide.\textsuperscript{85}

In June 2013, Tom Malaba, a journalist with the online news outlet Uganda Radio Network, was repeatedly followed by Rwandan agents and had his home raided after he attended a news conference in Kampala, during which he asked a question that ostensibly angered the Rwandan Ambassador to Uganda.\textsuperscript{86} Malaba had been investigating the plight of Rwandan refugees and sought clarification on allegations that the ambassador was behind a scheme to target Rwandan exiles in Uganda.\textsuperscript{87}

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.\textsuperscript{88} Worryingly, Andrew Muhanguzi, the brother of the editor of the Umuvugizi news website, John Bosco Gasasira, who lives in exile in Sweden, 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,\textsuperscript{89} but the Ugandan police stated they have no record of his arrest.\textsuperscript{90} 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.\textsuperscript{91}

Technical attacks against online news outlets and websites of human rights organizations are not common but have increased in recent years. In April 2014, the investigative news website, Ireme, experienced a seemingly targeted cyberattack, though the source of the attack was unknown.\textsuperscript{92}

\textsuperscript{85} Tom Rhodes, “Twitter war shines light on how Rwanda intimidates press,” Committee to Project Journalists (blog), March 24, 2014, \url{http://www.cpj.org/blog/2014/03/twitter-war-shines-light-on-how-rwanda-intimidates.php}.


Saudi Arabia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>32</td>
<td>33</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>70</td>
<td>72</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

| Population:                              | 30.1 million |
| Internet Penetration 2013:               | 60 percent   |
| Social Media/ICT Apps Blocked:           | Yes          |
| Political/Social Content Blocked:        | Yes          |
| Bloggers/ICT Users Arrested:             | Yes          |
| Press Freedom 2014 Status:               | Not Free     |

Key Developments: May 2013 – May 2014

- At least 35 news websites were blocked in December for failing to register with authorities, in the first signs that the government is enforcing e-publishing legislation passed in 2011 (see **Limits on Content**).

- Similarly, the General Commission for Audiovisual Media announced in April that it will begin monitoring YouTube videos produced in the country for compliance with local laws (see **Limits on Content**).

- A new anti-terrorism law criminalizes online expression that promotes atheism, insults the state’s reputation, harms public order, or threatens state security, among other things. Limits on arbitrary detention were also repealed, allowing security forces to detain individuals indefinitely and without charge (see **Violations of User Rights**).

- Prison sentences related to online activism and free expression have grown over the past year, with prominent human rights activists Mukhlif al-Shammari, Waleed Abu al-Khair, and Fadhel al-Manafes jailed for 5 to 15 years. Seven men from the Eastern province were sentenced to 5 to 10 years under the Anti-Cyber Crime Law for allegedly inciting protest and damaging public order through Facebook. They had been detained since 2011 (see **Violations of User Rights**).
Introduction

Tensions between technological advancement and religious dogma continue to characterize the online sphere in Saudi Arabia. Social media has opened a new space for public interaction between Saudis, even aiding in matchmaking between men and women in the conservative country. As use of Twitter and YouTube in particular reached some of the highest levels in the world, Saudis have employed online tools to highlight government corruption, discuss economic and social issues, and, in more limited cases, call attention to human rights violations. The government has responded positively to some low-level issues, but has shown a zero tolerance policy when red lines are crossed on political or religious issues.

Having first gained access to the internet in 1998, Saudis now go online from their home, place of employment, data-enabled mobile phones, and internet cafes. All forms of internet and mobile phone access are available in the country, including fiber-optic networks (FTTx), third-generation (3G) and fourth-generation (4G) mobile networks, internet via satellite, and High-Speed Packet Access (HSPA) technologies. In a sign that the government itself realizes the crucial role of Twitter, King Abdullah’s chief of royal court and gatekeeper, Khalid al-Tuwaijir, in March 2014 reactivated his defunct Twitter account. He indicated he would follow a list of 50 people at a time, asking them to send him requests or issues that needed to be resolved. However, while Saudi Arabia is a regional leader in providing e-government services, authorities have looked to exploit technology to more disturbing ends as well. A system whereby male guardians are alerted by text message when a woman leaves the country was introduced in November 2012. Following complaints from high-profile Saudi women, it was suspended in January 2014.

Public figures and religious authorities continue to warn citizens against the “evils” of social media and other online tools. On May 15, 2013, the country’s top cleric declared that a Saudi who uses Twitter “has lost this world and his afterlife.” In September 2013, it was reported that several government ministries warned that tweets are monitored and employees may face termination from their jobs for expressing critical opinions. Authorities have also stepped up the monitoring of social media, with the government announcing in April 2014 that it would begin to monitor YouTube videos produced in the country to ensure compliance with local laws. Dozens of news websites were blocked in February for failing to obtain a government license as the government took the first steps towards enforcing a law on online publishing passed in 2011.

While the country is grappling with regional threats related to the recruitment and return of armed extremists fighting in Syria, broad anti-terrorism regulations are being applied to human rights

---

defenders and critics of the state. In the Eastern Province (Ash-Sharqiyyah), where disparate protests have continued for years, seven men were sentenced for 5 to 10 years under the Anti-Cyber Crime Law for allegedly inciting protests and damaging public order through Facebook. A photographer known as the “Revolution’s Journalist” for documenting local protests was shot dead during a police raid on his neighbor’s home in February. Prominent human rights activists Mukhlif al-Shammari, Waleed Abu al-Khair, and Fadhel al-Manafes were jailed for 5, 10, and 15 years, respectively, in addition to extended travel bans and suspended sentences. Rai Badawi, the co-founder of the Saudi Liberals website that has been detained since 2012, had his jail sentence increased from 7 to 10 years in March 2014. The increased prosecutions come as the government passed new legislation that, among other things, equates the promotion of atheist thought with violent terrorism, and abolishes time limits on arbitrary detentions.

Obstacles to Access

Saudis have enjoyed a rapid growth of internet and communications technologies (ICTs) in recent years. Access had increased to 60.1 percent of the population by mid-2014, up from 36 percent in 2008. Fixed broadband subscriptions stood at 48.4 percent of all households, with a majority using ADSL connections. Monthly expenditure on 4G broadband ranges from between SAR 55 ($11) for a 2GB allowance to SAR 146 ($89) for a family plan of 60 GB. Household internet plus television packages with fiber-optic connections range from SAR 300 for speeds of 25 Mbps to SAR 800 for 200 Mbps.

Mobile broadband use is even higher, with a penetration rate of 78.3 percent. Standard mobile phone subscriptions have risen to 51 million, resulting in a penetration rate of 169.3 percent. Finally, 87.8 percent of mobile subscriptions are prepaid. The number of mobile users has dropped from a height of 54 million in 2011 as the government deported thousands of illegal workers and forced mobile companies to cancel free roaming service, thus cutting the number of SIM cards that were exported as well as deactivating prepaid cards whose owners are not registered.

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. Residents of provinces such as Jizan in the south and Ha’il in the north are the least likely to use the internet, while 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.

---

Saudi Arabia

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.

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 (Saudi Arabia), Mobily (owned by Etisalat of the United Arab Emirates), and Zain (Kuwait).

Internet cafes, once prevalent, have become less popular in recent years due to the broad availability and affordability of home broadband access. With the departure of many power users, internet cafes are now 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, all internet cafes must close by midnight, compliance of which is ensured by the police. 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.

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. In 2003, the Communication and Information Technology Commission (CITC) became responsible for providing internet access to the private sector.

The CITC establishes policies and enforces regulations on ICT services, including duties such as managing tariffs, performing content filtering, and licensing providers. Under the 2007 Anti-Cyber Crime Law, the CITC also assists the Ministry of Interior (MOI) in monitoring extremists and political activists. While both the CITC and KACST claim to enjoy administrative and financial independence, there is no evidence to support this. On the contrary, the CITC chairman is also the Minister of Communications and Information Technology, while the KACST President reports directly to the Prime Minister and is appointed by the King. Board members consist of government officials, appointed to these roles on the basis of their position within the government.

---


Limits on Content

The Saudi government continued to employ strict filtering over internet content throughout 2013 and early 2014. Authorities blocked dozens of news sites for failing to obtain a government license, the first time that regulations on online publishing, enacted in 2011, have been enforced. The General Commission for Audiovisual Media announced in April that it would begin to monitor Saudi videos uploaded to YouTube to ensure compliance with local laws. These moves reflect a growing regulation of online content, in line with authorities’ strict control over traditional media. Although high levels of social media use has translated into a growing diversity of content online, self-censorship remains prevalent when discussing topics such as politics, religion, or the royal family. Overall, these tools have also been used by ordinary citizens and human rights activists in order to raise awareness on issues surrounding poverty, gender inequality, and corruption. However, numerous arrests and lengthy prison sentences have had an overall chilling effect on online activism (See “Violations of User Rights”).

Past reports indicated that at least 400,000 websites that are considered immoral or politically sensitive are inaccessible within the country. 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. While part of the government’s blocking policy is designed to disrupt terrorist networks and the dissemination of extremist ideology, the government also blocks any content that it deems harmful to society or challenging to the royal family. Criticism of Saudi Arabia or 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. The extensive list of sites blocked under these policies is supplemented by an additional list formulated from recommendations by members of the public.

On March 13, 2014, the Ministry of Information announced it had blocked 35 unlicensed online publications. The websites were blocked for failing to obtain a government license under an online publishing law that was passed in January 2011, but not implemented until now. Abdelaziz al-Oqail, assistant undersecretary at the Ministry of Information and Culture, told al-Hayat on March 21 that another list of publications would be blocked, without providing more details. A spokesman from the Ministry of Culture and Information stated that any electronic newspapers that contained false information or offensive content, such as material that offended Islam, Saudi Arabia, or national traditions, would be shut down. Online publications must obtain a license from the Ministry of Culture and Information, which lasts for three years and can only be granted to citizens that have passed high school and are at least 20-years-old. Editors-in-chief must also be approved by the ministry.

In another bid to regulate online content, the General Commission for Audiovisual Media announced that it will begin to monitor YouTube videos made in Saudi Arabia for compliance with local laws. The president of the commission, Riyadh Najm, told the Wall Street Journal, “We will make them aware of what’s acceptable in Saudi Arabia… Criticism is acceptable as long as it’s professional and constructive.” Prohibitions would include nudity, alcohol, tobacco, and acts of a sexual nature, although it is still too early to how the government will censor in practice.

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 block 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.

The CITC also censors individual social media pages that demand political reforms or basic civil rights. These include the Facebook pages of Abdullah al-Hamid and Mohamed Saleh al-Bejadi, well-known Saudi human rights activists and co-founders of the ACPRA, as well as the Twitter accounts of Saudi human rights activist and blogger Nouf Abdulaliziz, Saudi journalist and political activist Muhana al-Hubail, and the head of the organization “Monitor of Human Rights in Saudi Arabia” Waleed Abo al-Khair. Authorities also blocked the official website for the “October 26th Women Driving campaign” on September 29th, 2013. One week later, a mirror site was also blocked. In early 2013, the government also temporarily blocked millions of Twitter pages in an experiment to test its capabilities.

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 did not restrict access to the controversial “Innocence of Muslims” video containing an offensive depiction of the Prophet Mohamed. Google later blocked the video in Saudi Arabia.

The CITC also has an aggressive stance toward Voice over Internet Protocol (VoIP) services that

25 According to the Alkasir.com, which provides information on blocked websites, the URLs acpra6.org and anhri.net are blocked in Saudi Arabia. See https://alkasir.com/map, accessed March 2, 2013.
30 See http://nofah.com/wordpress/.
31 See https://twitter.com/abualkhair.
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.\(^{35}\) 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 behind the short suspension.\(^{36}\)

There were several incidents in which pressure from social media users and online newspapers led to users deleting “controversial” tweets, disassociating themselves from their accounts, or even deleting their accounts. For instance, Twitter user Hesaah al-Sheikh disassociated herself from her account after public anger erupted over her tweet in which she equated listening to the singer Mohamed Abdo as listening to Allah.\(^{37}\) Disassociating oneself from a Twitter account is common in Saudi Arabia, particularly when simply deleting a controversial tweet is not enough to calm public anger. Users who are deemed to have acted inappropriately often publicly declare that the account does not belong to them and that another user is using their name to impersonate them, a common occurrence in Saudi Arabia.\(^{38}\)

These limitations 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.\(^{39}\)

The government responds to takedown notices from members of the public, who can use a web-based form to submit a complaint regarding undesirable material.\(^{40}\) Sites can also be unblocked through a similar process.\(^{41}\) Once an individual completes such a request, a team of CITC employees determines whether the request is justified. The manager of public relations at the CITC said the commission receives about 200 requests each day, though he would not comment on how often the CITC unblocks a site based on such an appeal.\(^{42}\) In one example, the CITC unblocked the website Mustamel after the owners obeyed a request from the CITC to remove illegal advertisements.\(^{43}\)

The government is somewhat transparent about what content it blocks. 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


\(^{38}\) “Saudi Minister of Culture and Information criticizes impersonation of intellectuals” [in Arabic], AlArabiya.net, March 2, 2013, [http://www.alarabiya.net/articles/2012/11/20/250707.html](http://www.alarabiya.net/articles/2012/11/20/250707.html)

\(^{39}\) “Raif Badawi’s wife provides ‘Anhaa’ with the list of charges against her husband and calls for his release” [in Arabic], Anhaa, April 25, 2013, [http://www.an7a.com/102662](http://www.an7a.com/102662).


blocked by the Information Ministry for licensing violations 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,\(^44\) and failure to abide by these bans may result in a fine of up to SAR 5 million ($1.33 million), according to Article 38 of the Telecommunication Act.\(^45\) 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.\(^46\)

After two years in which the space for moderate government criticism slowly opened, new anti-terror laws have had a chilling effect on users. Social media users are increasingly careful about what they post, share, or “Like” online. 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 Mohamed. 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. 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 manufacturing consent for its policies. It is believed the government employs an “electronic army” to constantly post pro-government views, particularly on social media. Pro-government 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.\(^47\) 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 searched 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.\(^48\)

Whereas the authorities provide monetary support to pro-government 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 to the ruling system. Numerous sites have been closed for copyright violations,\(^49\) or for featuring advertisements for drugs.\(^50\) In addition,


\(^{46}\) Saudis refer to this circumvention tool as a “proxy breaker.”


\(^{49}\) “CITC closed down Haraj site after advertising half kilo Hashish”, [in Arabic], AlSharq Newspaper, March 30, 2013, [http://www.alsharq.net.sa/2013/03/30/783097](http://www.alsharq.net.sa/2013/03/30/783097).

Saudi Arabia

several political opposition websites such as Humanf, Saudihr, Hummum, and Alwaqa have ceased operations in recent years, presumably because of pressure from the MoI.

While opposition blogs and online forums were once the main instrument for discussing political and social matters, most Saudis now use social media to share information and express opinions. According to Abdul Rahman Tarabzouni, the Head of Emerging Arabia at Google, Saudis collectively watch 190 million YouTube videos per day, the highest amount of views per capita of any country in the world.51 There are now dozens of comedic channels on YouTube, the most popular being “Eysh Elly,” “La Yekthar,” and “3al6ayer,” which respectively have around 126 million, 51 million, and 39 million total views.52 Omar Hussein, host of 3al6ayer, has touched on political issues and come out in support of women’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 rather than harsh criticism and their restraint against pushing the limits too far. 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.

In the past, the government turned a blind eye towards the online broadcasters.54 However, there are worries that government plans to monitor Saudi-made YouTube videos will result in self-censorship and pressure against users.

In limited cases, online activism has resulted in positive steps from the government. A YouTube video of a Saudi man abusing a foreign worker for speaking to his wife has reportedly prompted investigation from the government-sponsored Human Rights Commission.55 However, in the majority of cases, those who upload or are featured in controversial YouTube videos may face criminal charges. For example, three men were arrested in March 2014 for YouTube videos in which they urged the king to improve living standards.56 (See “Violations of User Rights”)

Similarly, Twitter continued to grow as a platform for expressing sensitive issues. Indeed, when interviewed, one Saudi described the country’s Twitter environment as a sort of virtual parliament “where people from all political sides meet and speak freely.”57 Saudis are the largest adopters of Twitter in the Arab world, with the number of users reaching 4.8 million, according to a report by PeerReach.58 Twitter is also a platform where victims of human rights abuses speak out in an effort to raise awareness and call for justice. Four Saudi princesses who say they have been locked up in

Saudi Arabia

isolation for 13 years have been active on the platform, resulting in international attention.\(^5^9\) Saudis have also used hashtags such as “Breaking the fences,”\(^6^0\) and “elected Consultative Council” to expose corruption by public officials or call for reforms.\(^6^1\) Prominent religious scholars, such as al-Awdah, have even contributed to these debates on Twitter.\(^6^2\)

On June 10, 2013, Saudi women took part in small “Sit-ins for Freedom” in several cities across the country in support of their detained relatives. Over 140 protestors were arrested in the two days that followed. The protests were organized the Twitter page @almonaseron, an advocacy group.\(^6^3\) On the occasion of Saudi Arabia’s National Day (September 23), online advocacy groups arranged protests using Twitter in Buraidah and other towns, where they demonstrated together with the families of prisoners of conscience, particularly members of the ACPRA.\(^6^4\)

Facebook is the third most visited site in the country\(^6^5\) with 7.8 million local users, according to a report by the Social Clinic in cooperation with The Loft Creative Hub.\(^6^6\) Over the past few years, Facebook groups have been active in organizing low-level demonstrations in cities throughout the country.\(^6^7\) However, more recently, the robustness of security forces in dismantling demonstrations and seeking out protestors for arrest has forced many Saudis to devise more creative forms of organized protest.

An online campaign, Saudi Nationality, has been started to change Article 7 of the Nationality Act, which grants only Saudi men the right to pass on nationality to their children. The children of Saudi mothers and non-Saudi fathers thus do not have access to public services.\(^6^8\) Online petitions have also been created to demand the release of political detainees, such as journalist and teacher Tariq al-Mubarak, who was arrested in October 2013 for supporting women’s right to drive.\(^7^0\)

The anonymous Twitter user @Mujtahidd continues to criticize high profile members of the royal

---

60 #ميطحت_كوبشلا
61 #سلجم_ىروش_بختنم
family,

and to provide detailed descriptions of state corruption. The popularity of the account has more than doubled over a short period, increasing from around 410,000 Twitter followers in June 2012 to over 1.5 million as of May 2014. In 2013, the user shared the tweets of dozens of users who defended the government using the exact same wording, thus evidencing the presence of a MoI Twitter army. Due to apparent insider knowledge, the Mujtahidd account is believed to be operated by a disgruntled member of the Saudi royal family.

**Violations of User Rights**

Saudi courts have passed some of the harshest prison sentences against online users in the world over the past year, 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. Authorities passed an anti-terrorism law that equates “insulting the reputation of the state” or “calling for atheist thought” with terrorism, allowing for the trial of numerous prisoners of conscience and human rights defenders in special terrorism tribunals under broad national security laws. Furthermore, a new law abolished time limits on arbitrary detention. Numerous Saudis have been detained for periods of months—and sometimes years—at a time without charge. Over the past twelve months, the cases of many of these victims were finally heard, only to result in lengthy prison sentences for expression that should be protected as a right.

Saudi Arabia has no constitution, but 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 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 assigns jail sentences and fines for defamation; the unauthorized interception of private email messages; the hacking of a website to deface, destroy, modify, or deny access to it; or simply the publishing or accessing of data that is “contrary to the state or its system.”

In late 2012, after an upsurge in defamation cases stemming from Twitter and the popular messaging service WhatsApp, the CITC deployed a large-scale media campaign to remind Saudis that “anyone who re-sends messages (via mobile phones and smartphone applications) that violate the sanctity of the private lives of citizens through insult, mockery, and violation of the sanctity of public morals, religious values and public order, will be sentenced to five years in jail, in addition to a fine of SAR 3 million ($800,000).” On August 8, 2012, the MOI also introduced a new web-based

---

74 [https://twitter.com/assaflovhotmail/status/307325546847694848/photo/1](https://twitter.com/assaflovhotmail/status/307325546847694848/photo/1).
form on its official website allowing internet users to complain about offensive comments made online about them.\textsuperscript{77}

Several laws passed over the coverage period have had a negative effect on the rights of internet users in Saudi Arabia. On November 22, 2013, King Abdullah approved amendments that removed a six-month limit on detaining individuals without court cases. The law, implemented in December, established a legal basis for infinite arbitrary detention.

On January 31, 2014, the Interior Ministry issued new anti-terror regulations that criminalized any form of association with banned religious or terrorist groups. Among many things, the law outlaws Saudis from fighting in wars abroad, an issue that came to the forefront as a result of the Syrian civil war. However, at home, the law defines terrorism in vague terms so that non-violent acts, such as “insulting the reputation of the state,” “harming public order,” or “shaking the security of the state” are criminalized as applicable offenses.\textsuperscript{78} Article 1 of the law defines “calling for atheist thought in any form” as terrorism.\textsuperscript{79} Article 4 of the anti-terrorism regulations makes it clear that promoting, expressing sympathy, or demonstrating affiliation with these banned groups includes “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.\textsuperscript{80}

The MoI introduced a new method for users to report offensive comments made toward them by other users, opening the door for an upsurge in defamation lawsuits that may ultimately have repercussions for freedom of expression. Overall, the MoI continues to enjoy relative impunity over its abuses of online users. Some have reported that authorities have confiscated their cars, computers, and other personal items indefinitely.

An alarming number of Saudi human rights activists, lawyers, and ordinary users were prosecuted over the past year, with disproportionately large prison sentences passed by the country’s terrorism tribunal. In general, outspoken bloggers face constant pressure by police authorities who engage in periodical interrogations and threats to initiate legal proceedings.\textsuperscript{81} On June 24, 2013, seven men from the Eastern province were sentenced to prison terms of 5 to 10 years and concomitant travel bans of the same amount of time for allegedly inciting protest and damaging public order through Facebook. They were convicted under Article 6 of the Anti-Cyber Crime Law, which deals with the creation, distribution, and storage of materials that “harm public order.” The men were first arrested in September 2011 and were held without charges until in April 2013, when their case came in front of a special anti-terrorism court.\textsuperscript{82}

\textsuperscript{77} “‘Interior’ confronts social networking sites abuse.. electronically”, [in Arabic], Aleqtisadiah Newspaper, March 9, 2013, http://www.aleqt.com/2012/08/08/article_681378.html


\textsuperscript{81} Interview with prominent blogger Foad al-Farhan, 2014.

\textsuperscript{82} According to Human Rights Watch, the seven individuals were Saleh al-Shaya’ (5 years), Hussein al Sulayman (7 years), Mohamed al-Khalifa (8 years), Mostafa al Mujahid (6 years), Hussein al-Bathir (5 years), Ali al-Hadlaq (7 years), and Abd al-Hamid al-Amer (10 years). See “Saudi Arabia: 7 Convicted for Facebook Postings About Protests,” Human Rights Watch, June 30, 2013, http://www.hrw.org/news/2013/06/29/saudi-arabia-7-convicted-facebook-postings-about-protests.
Saudi Arabia

On March 9, 2014, a Saudi appeals court upheld an eight-year sentence for a Saudi man found guilty of using Twitter and YouTube to call on detainees’ family members to protest. He was also convicted of “mocking” the king, religious officials, and government bodies.”83 One day later, another man was sentenced to 10 years in prison and a US$ 26,600 fine for encouraging protests on Twitter and using websites “hostile to the government and that promote deviant ideologies.”84 In both cases, the names of the men were kept anonymous and it was not clear when they were first arrested.

Twitter users who expose the misdeeds of government officials or public sector employees are often targeted by authorities. Well known human rights activist Mukhlif al-Shammari was sentenced to five years in jail in June 2013 for allegedly damaging the country’s domestic and international reputation, insulting religious bodies, and inciting discord. He was also banned from all media activity and cannot travel abroad for 10 years. He had written several articles and posted a video to YouTube in which two young girls described their mistreatment. In March 2014, he lost an appeal against the sentence.85

Three lawyers–Abdel Rahman al-Subehi, Bander al-Nakithan, and Abdel-Rahman al-Remaih–were referred to the public prosecutor in November 2013 after they had criticized the slow pace of judicial reform on Twitter.86 They were given prison sentences of five to eight years in October 2014 for charges relating to “insulting” and “interfering with the purview” of the ruler and the judiciary.87

In March 2014, three men were arrested for uploading separate YouTube videos in which they decried the economic situation in the kingdom and called on King Abdullah to distribute wealth in a more equitable manner. Mohamed Fahd al-Doussari was the first to post, with the other two videos made in support of his call after it was widely circulated on Twitter and other social media. All three individuals stated their full names and displayed their identity cards to the camera. According to activist Waleed Abu al-Khair, the individuals do not know each other in real life and are “just regular people” from different regions across the country.88

Well-known human rights lawyer Waleed Abu al-Khair was jailed on April 15, 2014 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.89 He was sentenced to 15 years–of which 5 years were suspended–and an ensuing travel ban of 15 years on July 6, 2014. He was tried under the Specialized Criminal Court, a terrorism tribunal. It is believed

he was targeted for statements he had made on Twitter and various media outlets related to the government's handling of prisoners of conscience.90

On April 17, 2014, blogger and activist Fadhel al-Manafes was sentenced to 15 years in prison and a fine of SAR 100,000 for “undermining national security and stability, inciting sedition and sectarian divisions, disloyalty towards the king, publishing articles and communicating with foreign journalists with the aim of harming the state’s image, and creating a banned association and inciting protests.” He had been held since October 2011. Al-Manafes is also a founding member of the Al-Adalah Center for Human Rights and maintains a blog that raises awareness of discrimination against the Saudi Shiite community.91

Victims have faced extended periods of arbitrary detention for their online activities. Hamza Kashgari, a young Saudi writer, was released in October 2013 after almost two years in detention without trial.92 He had been detained in February 2012 after publishing three tweets detailing an imaginary conversation with the Prophet Mohammed. Similarly, writer Turki al-Hamad was released on June 5, 2013 after spending five months in detention.93 He had been arrested in December 2012 after tweeting “...we need someone to rectify [the Prophet] Mohamed bin Abdullah’s doctrine.”94 Any discussion that questions an aspect of how Islam is practiced in society commonly leads to arrest. The incident inspired its own hashtag on Twitter and drew large amounts of both support and criticism.

Others who have been in detention for several years have been sentenced to lengthy prison sentences over the past year. Raif Badawi, co-founder of the Saudi Arabia Liberals website, had his sentence increased from 7 to 10 years in jail, as well as 1,000 lashes and a fine of one million Saudi riyals (US$ 266,000) in early May 2014.95 Badawi was charged with “setting up a website that undermines general security” and “ridiculing Islamic religious figures.”96 He has been held since 2012 and had been cleared of apostasy charges in 2013, which could have brought the death penalty. Also in May 2014, two bloggers that have been detained since 2012 were sentenced to long jail terms. Sheikh Jalal Mohamed Al-Jamal, who had been released in May 2013, was sentenced on an appeal to five years in prison and a SAR 50,000 (US$ 13,000) fine. His website, Awamia, was found to

have “attacked the Saudi state.” Ali Jaseb Touhifah was sentenced to six years and an identical fine. Touhifah has been detained since August 2012.\(^97\)

Aside from these arrests, there are a number of other cases that reflect the Saudi authorities’ strict control over free speech online. A young woman in Jeddah was questioned by the police because her Twitter profile carried the motto used in the Arab uprisings, “The regime has to fall.” Her father was asked to prevent her from tweeting, her mobile phone and laptop were confiscated, and she has to sign a pledge not to tweet.\(^98\) Tariq al-Mubarak, an online journalist and teacher, was detained by police on October 27, 2013, shortly after publishing an article on *Asharq al-Wasat*.\(^99\) The article was critical of religious extremists and the lack of freedoms in Saudi society.\(^100\)

A number of political activists remain imprisoned from previous years. On March 9, 2013, a court in Riyadh disbanded the human rights organization ACPRA 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.\(^101\) 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.\(^102\) Five founding members of ACPRA are also currently in detention.\(^103\) Two founding members of the Islamic Umma Party’, al-Wahiby and al-Gamidi,\(^104\) have been in prison since February 2011.\(^105\) Both the ACPRA and the Islamic Umma Party base many of their operations online.

Violent attacks against online users are rare, although in February a photojournalist named Hussein Ali Madan Al-Faraj was shot during a police raid. Al-Faraj was known as the “Revolution’s Journalist” for documenting protests and funerals in the Eastern Province, where Shi’ites form a majority. While the government claims they encountered violent resistance, other reports stated he had gone to document a heavy police raid targeting his neighbor. While the man was not home, both his son and Al-Faraj were killed by police.\(^106\)

New registration requirements have also undermined the ability to use ICT tools anonymously and free from government interference. As previously mentioned, the Ministry of Culture and Information requires that all blogs, forums, chat rooms, and other sites obtain a license from the Ministry to operate online, thus putting more pressure on online writers to self-regulate their

---


98 Interview with activists and human rights lawyers, 2014.


103 Those members are Suliaman Al-Rushoody, Mansour Al-Awth, Moussa Al-Garni, Mohamed Al-Bijadi and Saleh Al-Ashwan.


Saudi Arabia

content. Users are also 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.

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. 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, mobile phone text messages, and messages sent through the very popular service WhatsApp. 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.

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 legal 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.

As ICT use has grown across the country, the threat of cyberattacks has also escalated. Several government websites, including the Ministry of Interior were attacked in May 2013. A politically motivated hacker took down the website oct26driving.org in October, posting a threatening message in its place. In January 2014, 16 government websites were hacked by the Syrian Electronic Army.

Alarmingly, according to a report from the University of Toronto’s Citizen Lab, the government has coordinated with the Italian 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 linked to 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.\textsuperscript{115}

Singapore

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>N/A</td>
<td>Partly Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>n/a</td>
<td>6</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>n/a</td>
<td>14</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>n/a</td>
<td>20</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>N/A</td>
<td>40</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 5.4 million
Internet Penetration 2013: 73 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Authorities introduced and selectively applied new restrictions for online news providers, requiring ten of them to comply with takedown orders within 24 hours or risk forfeiting an SGD 50,000 performance bond (see Limits on Content).

- Three online news startups were subject to a new registration process requiring details about all staff, and prohibiting foreign funding (see Limits on Content).

- One online cartoonist was threatened with contempt of court charges for political content. One prominent blogger was charged under the same law; his case is still pending (see Violations of User Rights).

- The prime minister initiated defamation proceedings against a activist-blogger, the first time an individual blogger has been sued by a government leader; the case is pending (see Violations of User Rights).
Introduction

Singapore enjoys high and rising levels of digital connectivity. The internet has long been seen by the republic’s technocratic leaders as a critical part of the national infrastructure for economic growth and education. However, they are less enthusiastic about the internet’s potential for liberalizing political debate and enhancing democratic participation.

The People’s Action Party (PAP) government does not filter or block as a means of restricting political expression, but it does make use of sedition, defamation, and contempt of court laws to manage dissent. Officials initiated legal action against at least three bloggers during the coverage period. Based on a history of punitive charges under broadly worded legislation, most established blogs and news websites exercise a level of self-censorship, which varies based on their appetite for risk.

This self-censorship coexists with an unceasing flow of antigovernment comments online. The vigorous use of the internet by individuals and groups opposed to PAP dominance was cited as a key factor behind the ruling party’s setbacks in the 2011 general election. Ahead of the next election, expected in 2016, the government is exhibiting greater sensitivity towards online dissent. While its interventions are not severe enough to neutralize the internet’s importance as a space for alternative and more authentic voices, it may succeed in slowing down the growth of independent news sites and in discouraging more organized activism.

In particular, officials appear to be trying to forestall any emergence of professionally-run, independent online news organizations with substantial reach, as has happened across the border in Malaysia. During the coverage period, three digital news startups were required to provide extensive registration information and forego foreign funding. One that refused was then banned from engaging in any online activity. Separately, the government introduced a new regulatory framework for larger online news media, strengthening official powers to control content through takedown requests and levying a compliance-related bond. Though several sites could have met the framework’s criteria, it was selectively applied to just ten commercial platforms with the capacity to conduct independent news reporting; of those, just one appeared to fall outside the remit of existing media regulation. None of these platforms, whether startups or established outlets, hosted particularly combative or contested content, suggesting that this was part of a longer-term, preemptive strategy to suppress systematized independent reporting online.

Aside from these regulatory innovations, the government was also active in the use of traditional, offline legislative tools against bloggers. Although few in number, the cases sent a strong signal that the government had no intention of adopting liberal democratic norms for political discourse.

Obstacles to Access

As a wealthy and compact city-state, Singapore has highly developed information and communication technology infrastructure. Seventy-three percent of households had internet access in 2013, while mobile phone subscriptions outnumbered residents by 56 percent.¹ According to the

government telecommunications regulator Infocomm Development Authority (IDA), practically all households used broadband connections. Its Intelligent Nation 2015 master plan aims to establish an ultra-high-speed and pervasive network, with 90 percent home broadband usage by 2015. The fiber-based Next Generation Nationwide Broadband Network (Next Gen NBN) reached 95 percent of homes and businesses by July 2013. 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. In March 2014, the government announced that the number of hotspots would double to 10,000 by 2015.

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. In March 2014, the government launched an SGD 8 million (US$6.4 million) Digital Inclusion Fund to increase internet access in lower-income households.

The dominant internet service providers, which are also the mobile telephony providers, are Singapore Telecom (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 which, MyRepublic, launched a 1 Gbps broadband service in early 2014 at markedly lower rates than the incumbents.

The internet infrastructure is regulated by the IDA, a statutory body of the Ministry of Communications and Information (MCI), which 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. However, in 2013, the IDA approved the sale of the network company OpenNet, which is responsible for building and operating the passive infrastructure, to a unit of SingTel. Due to other players’ concerns that the acquisition was anticompetitive, the IDA required that SingTel sell off 75 percent of its stake in that unit by April 2018.

**Limits on Content**

The government has kept a 1996 promise not to block or filter any political content and has not subjected online media to the same level of discretionary licensing that restrict newspapers and

---


broadcasters. However, during the coverage period of this report, it strengthened its power to issue takedown orders to large commercial online news media, and imposed funding limitations on three fledgling internet news publishing companies. Both measures can be seen as a preemptive move against the future development of independent professional news sites that could seriously challenge the dominance of Singapore’s politically conservative mainstream media outlets, the way the online news organization *Malaysiakini* has in Malaysia. The government is expected to incorporate these powers into the Broadcasting Act in 2015.

The internet remains significantly more open than print or broadcasting as a medium for news and political discourse, which flow online largely unhindered. Any restraint of online discourse is mainly due to fear of post-publication punitive action—especially through strict laws on defamation, racial and religious insult, and contempt of court (see Violations of User Rights).

However, 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.” 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.

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 is known to comprise mainly pornographic sites and perhaps a few overseas sites run by religious extremists. In November 2013, the authorities took the unprecedented step of reaching beyond their list of 100 to block a controversial extramarital dating website, Ashley Madison. The Canadian company had declared its intention to launch in Singapore as part of its expansion into Asia, prompting complaints from conservative Singaporeans. The government said that the company “stands out” for its “flagrant disregard of family values and public morality” and as a site that “aggressively encourages and facilitates extra-marital affairs and has declared that it will specifically target Singaporeans.” Observers have noted

---

10 Broadcasting Act (Chapter 28) Section 3(5).
a trend of religious conservatives (mainly evangelical Christians) asserting themselves more in public morality debates, with politicians sometimes pandering to their demands for censorship.13

The MDA can also issue takedown notices for specific content. In July 2013, the government informed parliament that the MDA had issued a total of 24 takedown notices since 1996, an average of less than 1.5 per year. One was the 2012 *Innocence of Muslims* YouTube video, which several governments banned. Twenty-one were for pornographic content or advertisements for sex or sex chats, and two involved gambling. In February 2014, another site was given a takedown order for promoting drug use. The information minister said the MDA had never directed websites to take down content “just because it is critical of the Government.”14 However, several bloggers have publicly acknowledged removing critical content under threat of criminal prosecution or defamation suits (see Violations of User Rights), while others are widely believed to do the same behind the scenes. The scale of such self-censorship cannot be ascertained, but is most likely routine among journalists working online.

In June 2013, an individual licensing framework took effect for large online news sites, removing them from the class license outlined above. Sites brought under this new framework are required to comply with any takedown notice within 24 hours, and to put up a “performance bond” of SGD 50,000 (US$40,000) as an incentive to exercise best efforts.15 The bond is in line with the requirement for television niche broadcasters.16 The MDA said that the bond could be in the form of a banker’s guarantee, and that it was prepared to exercise flexibility if any site faced difficulty in complying with this requirement.17

The framework only 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. Ten news sites belonging to media corporations were considered to qualify. Seven are run by Singapore Press Holdings, the publisher of most of Singapore’s newspapers, while another two belong to the government-owned national broadcaster, MediaCorp. Newspaper, television, and radio companies are already subject to discretionary individual licensing and traditionally cooperate with government. Yahoo Singapore’s news site, the only one of the ten not belonging to national mainstream media, was the likely trigger for the new regulation. Yahoo News operates a small newsroom of full-time reporters dedicated to covering Singapore for a local audience on a daily basis. Previously unencumbered by any discretionary permit system, it was sometimes slightly bolder in its political coverage, which may have drawn policymakers’ attention to the regulatory loophole. However, neither it nor any of the other nine sites could be said to have had a track record of intransigence towards political pressure, and all

ty_in_Singapore.pdf.

14 “MCI’s response to PQs on Licensing Framework for online news sites,” Ministry of Communications and Information, July 8, 2013, http://www.mci.gov.sg/content/mci_corp/web/mci/pressroom/categories/parliament_qanda/mci_s_response_topgasonli-
censingframeworkforonlinenewsites.html.


16 “Fact Sheet – Online news sites to be placed on a more consistent licensing framework as traditional news platforms,” Media Development Authority Singapore, May 28, 2013, http://www.mda.gov.sg/AboutMDA/NewsReleasesSpeechesAndAn-

10 agreed to comply with the new system. Since it is unlikely that any of the 10 sites would disobey a takedown request, the full implications of the online licensing system—including whether refusal to comply would result in the unprecedented ban of a news site—may remain untested.

The new licensing framework was made public through a press release three days before it was implemented, highlighting the lack of transparent and politically independent processes for making or applying regulations.18 Bloggers and other observers complained that many of its details were unclear, including how the site’s audience was measured.

In parliament, the government denied that the new regulations were intended to stifle independent news coverage or criticism. It promised that the 10 sites would be consulted on the specifics of the licensing conditions to ensure that their operations would be virtually unaffected. Though prominent socio-political sites such as The Online Citizen qualified for the new licensing regime due to their large audience size and current affairs content the government said it was not considering extending the new rules to blogs that provide mainly commentary and did not perform regular original reporting.19 However, these assurances were not written into the regulations and only deepened unease about their arbitrary application.20

While this framework was designed for the largest news sites, the government’s other regulatory maneuver of 2013 targeted smaller start-ups with ambitions to go commercial. Most socio-political blogs generate negligible revenue and therefore lack the manpower to generate original reporting and commentary on a daily basis. However, a new start-up, The Independent, announced its ambition to develop a professionally run current affairs site.21 The team behind it included P. N. Balji, formerly editor of two national daily newspapers. Claiming that The Independent was on the brink of receiving foreign funding—which its owners denied—the government imposed new operating conditions on the company in July 2013.22 The publisher was required to sign an undertaking not to receive funds from foreign sources other than commercial advertising and subscription revenue. In addition, it had to submit detailed personal information about its owner, editorial team, and source of funds, including the names and national identity card numbers of individual funders, to the MDA. After some back-and-forth over the exact wording of the declaration forms, the group agreed to the terms.23

The same conditions were applied to Breakfast Network, another new online operation with a corporate existence and an editor-publisher with significant newspaper experience. In this case the publisher decided that the requirements were too onerous and opted to close the site rather than

---

register. In December 2013, the MDA issued a statement prohibiting the firm from operating “any iteration” of the website, including its Facebook page and Twitter feed. The owner responded by winding up the company, though the group’s Facebook page continues to operate. A third site, Mothership, was subject to the same funding and registration requirements in April 2014 and asserted. The site, which carries current affairs commentary along with humor and lifestyle stories, is owned by a social enterprise chaired by retired top civil servant Philip Yeo. Like Breakfast Network, it was not accused of courting overseas backers. Nevertheless, in each case, the MDA said that its structure as a corporate entity made it “more susceptible to coming under foreign influence through foreign funding.”

The new restrictions were built on preexisting regulations. There was already a registration system in place for sites deemed to be providing political or religious content, which required them to file with the regulator personal particulars, including the employment details, of the site’s owners and everyone involved in its operations. Through the years, a handful of sociopolitical sites were asked to register. Singapore’s first independent online magazine, Sintercom, closed down soon after registering in 2001, when its owner decided that registration implied an unreasonable degree of liability for the site’s content. However, most complied without being noticeably hindered. The revised registration process that the three start-ups were instructed to comply with in 2013-14 was more detailed and less transparent. While the older registration forms—like most other media license application forms—can be freely viewed on the MDA website, the new forms were not made public, prompting criticism that the regulator was practicing “arbitrary and confusing enforcement of the law.”

As for the foreign funding restrictions, these were first applied to online media shortly before the 2011 general election through separate legislation. The Online Citizen, the most active independent blog at the time, was not only ordered to register as a political site, but also declared a “political association” under the Political Donations Act of 2001, which banned it from receiving any foreign funding or anonymous local donations totaling SGD 5,000 (US$4,000) or more per year. The ban on foreign funding appears designed to close off the possibility of any Singaporean site replicating the formula of independent news website Malaysiakini, which had a major impact in neighboring Malaysia after startup funds from foreign foundations helped it become commercially viable. The three start-ups that the government singled out in the past year were not the most radical in Singapore’s cyberspace, but stood out for wanting to place citizen journalism on a financially sustainable footing.

Since government restrictions have been highly selective and intermittent, the blogosphere and social media environment remains vibrant. YouTube, Facebook, Twitter, and international blog-hosting services are freely available, and most bloggers are able to operate openly. Well-established independent sociopolitical blogs include The Online Citizen, TREmeritus and Yawning Bread. Their

---

ability to act as whistleblowers and watchdogs is hampered by the lack of any right to information laws and Singapore's plaintiff-friendly defamation law. They are also constrained by being almost entirely volunteer-run, with no capacity to engage in daily news reporting. Even before the government’s restrictions on fundraising, economic viability for independent online media was a remote prospect, due to the small market for political news. 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 on migrant worker rights and ACRES on wildlife protection.29

Overall, the main limitation on content results not from blocking, filtering, or takedown requests, but self-censorship by the main news sites and blogs. Self-censorship is prompted partly by fear of the strict application of defamation, contempt of court, and other laws (see Violations of User Rights). Executives of larger media houses may also dread losing the PAP's 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. As a result, news websites run by major media houses tend not to deviate significantly from the official line on controversial political issues. Universities and think tanks are not known to offer radically divergent views either.

On online forums and social media, by contrast, 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 have at best narrowed the gap with its critics rather than extending its unfair offline advantage into the online space.

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 major role in voicing public opposition to the government’s early 2013 Population White Paper, which planned for a large immigration-led population increase to 6.9 million in 2030.30 Facilitated by online publicity, activists organized a series of rallies at Hong Lim Park, the only venue where outdoor gatherings are allowed without a permit. The reaction forced the government to sidestep the population projection in February 2013.31 Another online campaign protested against long-established rules prohibiting female police officers and nurses from wearing the Muslim head-cover, the hijab, as part of their uniforms. The pressure was sufficient for the prime minister and other cabinet ministers to meet with selected community leaders in January 2014 and promise that the government’s position would gradually evolve.32

---

The news website licensing framework triggered a #FreeMyInternet campaign during the coverage period of this report.\(^{33}\) Most independent bloggers participated, but it did not succeed in changing the government's mind. The campaign also responded to the MDA's actions against *The Independent* and *Breakfast Network*, and issued a statement in late 2013 warning that "the future of Singapore's online space remains in jeopardy from being regulated by those who do not appear to know what they are doing, and whose intentions remain unknown."\(^{34}\)

## Violations of User Rights

While citizens are relatively 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 political opposition. During the coverage period, the prime minister sued a blogger for defamation, while another blogger faced contempt of court charges. Police briefly detained an online cartoonist for possible sedition and charged him with contempt of court, though proceedings against him were later dropped. The authorities are believed to exercise broad legal powers to obtain personal data for surveillance purposes in national security investigations, and in the past year, a government website began encouraging citizens to register before posting comments.

The republic's constitution enshrines freedom of expression, but also allows parliament wide leeway to impose limits on that freedom.\(^{35}\) 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 in 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.\(^{36}\) Punishments for first-time offenders could include a jail term of up to three years. Newer provisions in the penal code 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."\(^{37}\) Singapore's first cases of imprisonment for online speech were under the Sedition Act in 2005, when one citizen was sentenced to a month in jail and a second for a day for online postings insulting Muslims.\(^{38}\) This was also the first prosecution under the Sedition Act since independence in 1965. One of the side effects

---

\(^{33}\) "#FreeMyInternet – Movement against new licensing requirements for online media," *The Online Citizen*, June 1, 2013, [http://www.theonlinecitizen.com/2013/06/movement-against-new-licensing-requirement-for-online-media/](http://www.theonlinecitizen.com/2013/06/movement-against-new-licensing-requirement-for-online-media/).


\(^{35}\) Constitution of the Republic of Singapore, Section 14.

\(^{36}\) Sedition Act (Chapter 290) Section 3.

\(^{37}\) Penal Code (Chapter 224), Section 298.

of Singaporeans’ free access to social media, bypassing experienced mainstream media gatekeepers, is that members of the public now have more occasion to take racial or religious offense at content circulating in the public sphere. Police investigations into these complaints appear to be a regular occurrence, but rarely result in prosecutions, and none were reported in the period under review. In most known cases, police intervention at an early stage has been enough to elicit apologies that satisfy the targets of the offending expression.

Defamation is criminalized in the penal code and punishable with a jail term of up to two years. 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 region of SGD 100,000 to 300,000 each (US$80,000 to US$240,000) in defamation suits brought against opposition politicians and foreign media corporations. Electronic media have been on the receiving end: 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$477,000). 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 2013, Singaporean cartoonist Leslie Chew was arrested over his satirical cartoon strip, Demon-Cratic Singapore, which he publishes on Facebook. The offending cartoon contained a thinly veiled attack on the “racist government” of the fictional “Demon-critical Singapore”, including a leader who “abhors Malays”. He was held in custody for two days as part of an investigation into possible offenses under the Sedition Act before being released on bail. The Attorney-General’s Chambers (AGC) dropped that line of inquiry in July 2013, but charged him with contempt of court for scandalizing the judiciary. The AGC dropped the case in August 2013 when Chew took down offending strips and apologized.

---

39 Penal Code (Chapter 224), Sections 499-500.
In an unrelated case, blogger Alex Au faced contempt of court proceedings for the second time in two years. In the first incident, the AGC alleged in 2012 that he had scandalized the judiciary in a post arguing that “police, prosecutors and judges are more indulgent towards the well-connected.” Au acceded to the AGC’s demand that he take down the post and apologize.47 However, he followed it up with a critique of Singapore’s contempt laws, through which, he said, the executive had “effectively given our judiciary a blank check to be mercenary, biased, lazy and incompetent.”48 More than a year later, in November 2013, the AGC again accused Au of scandalizing the judiciary in two recent posts.49 Au is contesting these latest charges, for which the maximum penalty is two years in jail for each offense. Following his lawyers’ advice, Au removed the two blog posts. At the end of the coverage period, the case was headed to court.50

Official intolerance of political speech was most notable in May 2014, when Prime Minister Lee Hsien Loong sued activist Roy Ngerng for defamation. 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.51 After the government announced a tightening of CPF withdrawal rules, Ngerng 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.52 Ngerng apologized and offered to pay damages of SGD 5,000 (US$4,000). Lee’s lawyers rejected this as “derisory”, adding that Ngerng could be liable for aggravated damages as he had emailed similar allegations to the media even after apologizing.53 Defamation proceedings commenced at the end of the coverage period. An open letter to the prime minister, signed by more than 50 citizens including prominent activists and bloggers, called for greater respect for freedom of expression and argued that his threat of legal action was “an oppressive tool with undue chilling effects on public discourse”.54 Marking the first time that an individual blogger was being taken to court for defamation by a government leader, the case was seen by commentators as evidence of a souring of relations between the ruling party and critical segments of the public.55

---

A more positive recent development is the emergence of a small handful of Singaporean lawyers prepared to take on human rights and other public interest cases, including M. Ravi, Peter Low, and Choo Zheng Xi. This increases the likelihood of defendants claiming trial, and opens up the possibility of the court system making incremental advances towards greater freedom of expression. When blogger Han Hui Hui faced the threat of legal action from the Council of Private Education over emails she sent to the media alleging that the body had lied to reporters, her lawyer Ravi helped her apply to the courts for a declaration that a government body was not entitled to sue an individual for defamation. Although the dispute was settled, Han and her lawyer said that they would persist in their effort to get a High Court declaration on this legal question.\(^{56}\) Ravi is also representing Ngerng.

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. The owner of Breakfast Network declined to register because the MDA required the names of anyone involved in the “provision, management and/or operation of the website,” including volunteers.\(^{57}\) Starting from December 2013, the government’s main citizen consultation portal, REACH, required users to log in to their Facebook accounts before posting comments, in the belief that anonymity was encouraging irresponsible behavior on the site. Government leaders said they hoped the example would encourage the owners of other Singaporean discussion platforms to follow suit, but have not required it.\(^{58}\)

Even without registration, surveillance is “an accepted but hidden fact of life” and “few doubt that the state can get private data whenever it wants,” as one technology blog put it.\(^{59}\) Under the sweeping Computer Misuse and Cybersecurity Act, for example, 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.\(^{60}\) Court permission need not be sought. Failure to comply with such orders is punishable with a fine of up to SGP 50,000 (US$40,000), 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.\(^{61}\) No warrant or special authorization is needed. Penalties for non-compliance can include a fine of up to SGP 5,000 (US$4,000), 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$8,000), jail terms up to three months, or both.

---

60 Computer Misuse and Cybersecurity Act (Chapter 50A) Section 15A.
61 Criminal Procedure Code (Chapter 68) Section 39.
In August 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, 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 in the past year. 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. The Personal Data Protection Act enacted in 2012, which comes into force in July 2014, exempts public agencies and organizations acting on their behalf.

There were no violent incidents targeting internet users in the past year, though trolling and cyber harassment have emerged as major concerns in official circles as well as among many internet users. A section of the Straits Times website that reported on government websites being hacked was itself attacked in November 2013, by a hacker using the moniker of the global hacktivist collective Anonymous. A new Protection from Harassment Bill was passed by parliament in March 2014, covering online as well as offline and face-to-face communication. It provides both criminal and civil remedies for victims of harassment, alarm, or distress. Where the offense is intentional, possible sanctions include a fine of SGP 5,000 (US$4,000) and six months’ imprisonment. Civil remedies include protection orders and factual corrections of false statements.

---


South Africa

### Internet Freedom Status

<table>
<thead>
<tr>
<th>Category</th>
<th>2013</th>
<th>2014</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>8</td>
<td>8</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td><strong>TOTAL</strong> (0-100)</td>
<td>26</td>
<td>26</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population:</td>
<td>53 million</td>
</tr>
<tr>
<td>Internet Penetration 2013:</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 2014 Status:</td>
<td>Partly Free</td>
</tr>
</tbody>
</table>

### Key Developments: May 2013 – May 2014

- A new broadband policy called South Africa Connect was initiated in December 2013, with aims to provide every citizen access to a broadband connection at a cost of 2.5 percent or less of the average monthly income by 2020. This policy was complemented by the rollout of broadband plans in provinces like Gauteng, which aim to provide free internet access to the poor (see [Obstacles to Access](#)).

- There were no incidents of online censorship in South Africa during the coverage period, though video clips from a new satellite news channel posted on YouTube were taken down for alleged copyright violations in August 2013; some speculated political motivation behind the requests (see [Limits on Content](#)).

- While the online sphere is becoming a dominant source of news and information for South Africans, acquisitions by politically-aligned companies of major news outlets and the launch of new media products by pro-ANC businesses indicated the government’s growing influence in the media (see [Limits on Content](#)).

- The General Intelligence Laws Amendment Bill, enacted in July 2013, provides state security agencies with an ambiguous authority to intercept “foreign signals intelligence” without judicial oversight (see [Violations of User Rights](#)).
South Africa

Introduction

The digital media environment in South Africa can be described as generally free and open. A culture of free expression exists online, with diverse content available. Moreover, potentially significant moves by the government, such as the passage of a new broadband policy and funding of at least one major public access broadband initiative, suggests a positive trend toward access to the internet generally, especially for the poor. Access is a core concern for both civil society and the private sector, and in this regard, there has been an effective collaboration of interests between public and private players. While the Telkom monopoly remains a challenge in reducing overall landline costs, and there remains a general perception that mobile operators overcharge to maximize profits, public calls for a strengthening of the communications regulator to pay attention to these challenges are positive signs.

The online sphere remains diverse and active in South Africa, and marginalized communities are projected to benefit from new access initiatives over time. However, there is little evidence that the industry as a whole—including service providers, internet intermediaries, and media houses—is building a media environment based on principles of human rights and constitutional rights. The cost of access remains high, largely from profiteering and monopolistic practices, and intermediaries err on the side of caution when it comes to takedowns requests of illegal content. In August 2013, several video clips of on-air blunders from the newly launched African satellite news channel, Africa News Network 7 (ANN7), were taken down from YouTube for alleged copyright violations, though some speculated political motivation behind the requests. Meanwhile, acquisitions by companies of major news outlets aligned with the ruling African National Congress (ANC) ruling party and the launch of new media products by pro-ANC businesses during the coverage period indicated the government’s growing influence in the media.

The Protection of State Information Bill (POSIB), or so-called “Secrecy Bill,” made movements toward becoming law in 2014, threatening to criminalize the possession and distribution of state information, including online. Government surveillance powers increased with the passage of the General Intelligence Laws Amendment Act (or “Spy Bill”) in July 2013, which ambiguously provides security agencies authority over communications from foreign servers without judicial oversight. Meanwhile, government requests for user data from Google and Facebook increased over the past year.

Obstacles to Access

Although internet penetration has expanded rapidly in South Africa, in part due to the EASSY and SEACOM fiber-optic cables, many believe that this expansion has not been fast enough for the socioeconomic development needs of the country. Nonetheless, the internet is steadily spreading across the country, with 49 percent of the South African population having access by the end of 2013, up from 41 percent in 2012, according to the International Telecommunication Union (ITU).1 A recent household survey released in August 2013 by Statistics South Africa, the official statistics body in the country, stated that 41 percent of households have at least one member of

---

South Africa

the household who has access to the internet, whether at home, work, or at other locations such as internet cafes. However, access tends to fall along socioeconomic lines, with less than 10 percent of South African households enjoying the internet at home.²

Most internet users access the internet from their mobile phones,³ as fixed-line broadband reached only 3 percent of the population in 2013.⁴ By contrast, mobile phone penetration is 148 percent⁵ as a result of separate subscriptions for voice and data services.⁶ According to ITU estimates, over 25 percent of South Africans have access to mobile broadband.⁷ Meanwhile, the average internet connection speed in the country is 2.6 Mbps (compared to a global average of 3.9 Mbps), according to May 2014 data from Akamai’s “State of the Internet” report.⁸ In addition, South Africa’s broadband adoption (characterized by connection speeds greater than 4 Mbps) is about 8 percent of the internet population, while the country’s narrowband adoption (connection speeds below 256 kbps) is 2 percent.⁹

In an attempt to reach its universal service targets, the government, via the Universal Service and Access Agency of South Africa (USSASA), has launched various access initiatives since 1994 such as telecenters and multi-purpose community centers (now called Thusong centers). In December 2013, the Department of Communications implemented a new broadband policy called South Africa Connect, which aims to provide every citizen with access to a broadband connection at a cost of 2.5 percent or less of the average monthly income by 2020.¹⁰ The policy also aims to give 90 percent of South Africans access to a minimum speed of 5 Mbps.

In February 2014, the Gauteng provincial government awarded a ZAR 1.5 billion (US$135 million) tender to develop the Gauteng Broadband Network to service 316 government owned buildings, 45 Thusong centers, 9 economic development zones, and 20 townships in the province. Access to the internet at these points is expected to be free, with 95 percent of the province’s population connected to high-speed broadband following the completion of the 1,600 kilometer fiber-optic cable network in 2019.¹¹

There are hundreds of ISPs in South Africa, with 170 ISPs belonging to South Africa’s ISP Association

---

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 International Telecommunication Union, “Fixed (Wired)-Broadband Subscriptions, 2000-2013.”
⁵ International Telecommunication Union, “Mobile-Cellular Telephone Subscriptions, 2000-2013.”
South Africa

(ISPA), though the fixed-line connectivity market is still dominated by the Telkom monopoly—a partly state-owned company of which the government has a 39 percent share and an additional 10.5 percent share through the state-owned Public Investment Corporation—despite the introduction of a second national operator Neotel. By mid-2013, Neotel was reported to have 3,000 business customers and 152,000 consumer customers, compared to around 4 million customers using Telkom’s service.

Meanwhile, 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. Prices for mobile services are relatively expensive, while the quality of mobile services is reportedly low. As pointed out by the research firm World Wide Worx, data charges as high as ZAR 1-2 (US$0.10-0.20) per megabyte has resulted in South Africa’s mobile internet uptake falling behind other African countries, such as Nigeria and Kenya. South Africa’s mobile affordability ranked 33rd out of 44 African countries surveyed by Research ICT Africa in 2012 for the cheapest price available from dominant operators.

While the market for telecoms is fairly open, cybercafes face regulatory controls that impact their economic viability. Pursuant to Section 27(A)1 of the Electronic Communications Act, internet service providers (ISPs) and internet cafes are required to register with the Film and Publications Board (FPB), which falls under the Department of Home Affairs and is a relic, albeit a reformed one, of the Apartheid publication censorship regime. The registration requirements are not unreasonably onerous, though failing to register is an offence that may be subject to a fine, six months of prison, or both. Although many internet cafes do register with the board, there is little public evidence of enforcement.

Access providers and other internet-related groups are self-organized and quite active in lobbying the government for better legislation and regulations. The autonomy of the regulatory body, the Independent Communications Authority of South Africa (ICASA), is protected by the South African constitution, although several incidents in 2011 involving ministerial policy directives sent to the regulator have called into question the extent of its independence. In 2013, the Open Society Foundation conducted a review of ICASA, which found that while the institutional structure of the

14 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.
18 The applicant needs to provide his or her name, business name, national identification number, address and contact details, and nature of his or her business. The cost of registration is ZAR 462 (US$47). See, Internet Service Providers Association, “ISP/IP-Cafes Training Course,” January 2011, http://bit.ly/1bnOTP5.
regulator, including in its independence from the state, is strong, the regulator lacks leadership and independence, including financial independence, for it to be fully functional.

Limits on Content

There were no incidents of online censorship in South Africa during the coverage period, though video clips from a new satellite news channel posted on YouTube were taken down for alleged copyright violations in August 2013. ANC-aligned businessmen made significant inroads into the media landscape by acquiring and launching new media products over the past year, indicating the government’s growing influence in the media.

Internet content and social media platforms remain mostly free from government censorship and interference in South Africa. YouTube, Facebook, Twitter, and international blog-hosting platforms are freely available.

The Electronic Communications and Transactions Act of 2002 (ECTA) requires ISPs to respond to take-down notices regarding illegal content such as child pornography, defamatory material, or copyright violations. Members of the Internet Service Providers’ Association (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 appeals mechanisms for content creators or providers. The Department of Communications has suggested improving this with a new ECTA provision that would allow a service provider to respond to the grounds of a complaint before acting upon a notice. The complainant could then reconsider and decide to withdraw the notice or send a final takedown request that would obligate the service provider to act or lose its protection from liability. This proposed mechanism, however, still falls short of an actual appeals process, which remained absent as of mid-2014.

The Film and Publications Board (FPB) also regulates media and internet content in South Africa, the most recent report of government interference on freedom of expression online occurred in September 2012, when the Constitutional Court upheld a 2011 Gauteng High Court judgment ruling the controversial 2009 amendments to the Films and Publications Act of 1996 unconstitutional, based on the conclusion that the prescreening of publications (including internet content) would affect the value of news and be an unjustifiable limitation on freedom of expression. Before the Constitutional Court ruling, an art gallery successfully appealed the classification of a controversial painting of President Jacob Zuma known as “The Spear,” which the ruling party tried to ban from public display and dissemination online. See, “South Africa,” Freedom on the Net 2013.

21 The Ministry of Communications has recognized the association as an industry representative body under the act. The association acts as an agent on behalf of its 160 members and provides the ministry with annual information about the total number of take-down notices issued, the actions taken in response, and the final results. Most of the complaints lodged are resolved amicably, with ISPA’s clients agreeing to take down the offending content.


though it has departed dramatically from its Apartheid-era predecessor’s censorship activities. Today, the FPB focuses on content classification only. Critics, however, have pointed to the FPB’s broadening powers following several amendments since 1996, when the body was created, 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. Nonetheless, in its 2013-2018 Strategic Plan published in January 2014, the FPB recognized its “limited capacity and procedures for the regulation of content distributed online and mobile platforms” and accordingly outlined a plan to implement the requisite infrastructure needed to “establish an efficient and effective online and new media content regulatory strategy for the country.”

In August 2013, several video clips of on-air blunders from the newly launched African satellite news channel, Africa News Network 7 (ANN7), were taken down from YouTube after they were uploaded by members of the public. Although the takedown requests cited copyright violations, some speculated political motivation behind the requests, given that ANN7 is controlled by the powerful Gupta family from India, whose business dealings in South Africa and proximity to President Jacob Zuma have come under intense public criticism.

While copyright violations comprise the majority of takedown requests, Google’s most recent transparency report from the January to June 2013 reporting period noted that the platform had received five court orders to remove eight items from its Blogger and Google+ services for content related to bullying or harassment. Google also reported that it had received one request “from the Counter Intelligence Agency to remove a blog post that allegedly infringed copyright by criticizing a media release that the agency had issued.” The platform did not comply with any of the requests from that period.

Online self-censorship is low in South Africa, and the government does not actively try to limit or manipulate online discussions. Nevertheless, the ANC-led government frequently complains about antigovernment media bias, and in response, ANC-aligned businessmen have made significant inroads into the media landscape by acquiring or launching new media products over the past few years. Most recently, the Independent News & Media consortium, which has over 13 mainstream newspapers under its belt, was bought by Sekunjalo Investment Holdings, a company that is said to be highly politically connected. Other shareholders in the acquisition included two Chinese companies, possibly as part of China’s supposed “soft power” strategy of influence in Africa.

Citizens are able to access a wide range of viewpoints and perspectives online. Web-only news

24 The FPB’s motto is: “We inform, you choose.”
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 relying on the internet and radio for information and are depending less on television and print news for current affairs.\(^\text{30}\) Similarly, there are indications that in rural areas with internet access, the online versions of community newspapers, rather than their print versions, are being accessed ahead of the print publication.\(^\text{31}\) 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.

There are a number of political and consumer-activist websites, though the internet is not yet a key space or tool for social or political mobilization. Nevertheless, individuals and groups openly express their views via email, instant messaging, chat rooms, and social media, while the South African blogosphere has become highly active in discussing issues such as HIV/AIDS and the environment. The internet and mobile phones are increasingly used for political organization, as seen during the protests and activism against the controversial Protection of State Information Bill (POSIB) in 2012 and 2013, which President Jacob Zuma vetoed based on questions of its constitutionality and sent back to the National Assembly for reconsideration in September 2013.\(^\text{32}\) (The bill was subsequently revised and sent back to the president for his signature, which is still outstanding as of mid-2014. See “Violations of User Rights.”)

### Violations of User Rights

A so-called “Secrecy Bill” made movements toward becoming law in 2014, threatening to criminalize the possession and distribution of state information, including online. Government surveillance powers increased with the passage of the General Intelligence Laws Amendment Act (or “Spy Bill”), which ambiguously grants security agencies authority over communications from foreign servers without judicial oversight. Meanwhile, government requests for user data from Google and Facebook grew.

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.”\(^\text{33}\) The judiciary in South Africa is independent and has issued a few rulings protecting online freedom of expression in recent years. 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.\(^\text{34}\)

---

\(^{30}\) 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.


In November 2013, the Protection of Personal Information Act was signed into law, enacting 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-2014.

One piece of legislation debated throughout the coverage period—the Protection of State Information Bill (POSIB), also known as the “Secrecy Bill”—threatens to infringe on freedom of expression, press freedom, and internet freedom, if passed. In general, POSIB aims to implement a system to regulate state information, but instead places 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, would be held criminally liable and face up to 10 years in prison. Adopted by the National Assembly in November 2013, the bill still awaited President Jacob Zuma’s signature as of mid-2014. Opposition parties have called the bill an “assault” on democracy, while numerous civil society groups, including the South African National Editor’s Forum (SANEF) and the Right2Know campaign, have actively protested the bill.

The right to anonymous communication is compromised by legislation known as the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA), which requires 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. As many people in South Africa do not live in formal housing, this can be an obstacle to mobile phone usage.

The interception of communications is explicitly prohibited under RICA, unless permission is received from a judge designated to rule on the practice, which includes guidelines for judges to establish whether the interception is justified in terms of proportionality and narrowly defined standards. RICA also requires ISPs to retain customer data for an undetermined period of time and 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 interception. Nonetheless, civil society organizations have called for greater transparency in RICA’s

---

implementation. Meanwhile, internet cafes are not required to register users or monitor customer communications.

Government surveillance has become a growing concern in South Africa, particularly following the passage of the General Intelligence Laws Amendment Act (known locally as the “Spy Bill”) in July 2013, which originally intended to formalize the monitoring and interception of foreign signals (electronic communications stemming from abroad) without oversight. Prior to its passage, judicial permission was only required for the surveillance of local communications under RICA, which meant that state security apparatuses could monitor foreign signals (including on servers belonging to Facebook and Google) without any form of oversight. In response to civil society pushback against the “Spy Bill,” the final version signed by the president in July omitted all mention of “foreign signals,” creating concern that the exclusion would allow security agencies to continue to intercept foreign communications without any judicial review.

Meanwhile, the National Communications Centre’s (NCC) surveillance of mobile phone conversations, SMSs, and emails continues to raise a level of criticism from the media for its lack of transparency. The NCC also has the technical capacity and staffing to monitor both SMS and voice traffic originating 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.

In June 2013, critical analysis by the Mail & Guardian newspaper stated that the NCC “remains largely unregulated and free of oversight, while Parliament continues to fret about what its legal status should be.”

Government requests for user data on international communications platforms have been on the rise in recent years. Between July 2013 and June 2014, a total of nine requests were made by the government for information on nine separate user accounts on Google; none of these requests were granted. Similarly on Facebook, a total of five requests for five different user account information were requested between July 2013 and June 2014, none of which were granted.

Revelations in April 2013 that FinFisher spyware was being used by the partially state-owned Telkom

---

to intercept private communications have fueled further concerns of government surveillance.\textsuperscript{51} In many other countries, such servers have been used to harvest data and user information such as “screenshots, keylogger data, audio from Skype calls, passwords and more” collected by the spyware suite.\textsuperscript{52} While Citizen Lab also found evidence of FinFisher being deployed by the authorities in Ethiopia and used against political dissidents in Bahrain,\textsuperscript{53} the extent to which FinFisher has been implemented in South Africa and by what entities was unknown as of mid-2014. In January 2014, the government was reported to have funded the South African IT company VASTech to develop unknown surveillance technology with intentions to sell to Libya.\textsuperscript{54} According to the Privacy International report, the export of surveillance technologies is not regulated in South Africa.

There have been no reports of extralegal intimidation targeting online journalists, bloggers, or other digital technology users by state authorities or any other actor. Cyberattacks have recently become a growing issue in South Africa, and these are criminalized under the Electronic Communications and Transactions Act of 2002 (ECTA). Government websites have been hacked in the past, with the website of the South African National Road Agency Limited (SANRAL) most recently attacked. SANRAL is responsible for the controversial rollout of an e-tolling road fee system in Gauteng. In the attack, a security flaw was exposed that could give hackers access to the personal details of registered road users. According to SANRAL, the attacks disabled its website’s international access.\textsuperscript{55} In August 2013, a suspected hacker exposed a security flaw on the website for the City of Johannesburg’s online e-statement system.\textsuperscript{56} Also in August 2013, MTN was subject to a DDoS attack which had pulled down its servers, affecting its clients for a day.\textsuperscript{57}

Cybercrime has long been a challenge in South Africa, with a 2013 Norton Report ranking South Africa as the country with the third-highest number of cybercrime victims, following Russia and China.\textsuperscript{58} A National Cyber Security Advisory Council was set up in October 2013 as mandated by the 2012 National Cyber Security Policy Framework, which aims to coordinate business, government, and civil society actions against cyberattacks and crimes. In addition, so-called “cyber inspectors” have been mandated by the ECTA, though these inspectors do not require any specific qualifications (a point of criticism from activists and industry members), and the concept has not been properly implemented, ostensibly due to a skills shortage.\textsuperscript{59}

53 Morgan Marquis-Boire et al., “For Their Eyes Only”
## South Korea

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partly Free</td>
<td></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>13</td>
<td>14</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>32</td>
<td>33</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

### Key Developments: May 2013 – May 2014

- Prosecutors indicted the former head of national intelligence on the charge of orchestrating more than one million tweets and online comments in favor of the ruling conservative party in the December 2012 presidential election (see Limits On Content).

- Government agencies requested broadcasters and isps cooperate with ministers to downplay negative criticism online following a ferry tragedy with over 300 casualties in April 2014; lawmakers proposed criminalizing rumors during disasters (see Limits On Content).

- In August 2013, some lawmakers proposed enhancing criminal penalties for defamation committed online, which are already more severe than those outlined in the penal code (see Violations of User Rights).

- At least three people were sentenced for defaming President Park Geun-hye online, one to an 18-month prison term (see Violations of User Rights).

- In January 2014, conservative lawmakers proposed legally mandating the installation of mobile surveillance technology by telecommunications companies, who already share user data with government agencies (see Violations of User Rights).
Introduction

Users of South Korea’s advanced digital infrastructure faced new challenges as well as longstanding restrictions during the coverage period of this report. As Park Geun-hye of the conservative Saenuri Party entered her second year as president,1 prosecutors were investigating intelligence and military agents accused of manipulating online conversations to ensure her victory in the 2012 election.2 Even while these supposedly neutral agencies were accused of partisanship, lawmakers sought to give them more powers to monitor citizens’ digital communications.

Affordable, high-speed internet in South Korea’s vibrant fledgling democracy comes with a unique set of restrictions.3 Internet users face censorship rooted in political tensions with North Korea or traditional social values, and numerous laws regulate different aspects of digital activity. Observers say these restrictions have increased under the conservative party.4 In June 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.5

Criminal investigations targeting internet users are of particular concern. Twitter user Park Jung-geun retweeted posts from a North Korean account as a joke, then spent a month in detention and two years in court before his conviction and suspended jail term for promoting anti-state activity was overturned on appeal in August 2013. Other courts sentenced at least three people for defaming the president on the internet in the past year, including one to eighteen months in prison in November 2013. Officials sought to introduce heavier criminal penalties for online defamation, which South Korean law already punishes more severely than its offline counterpart.

Online privacy was the other prevailing issue for South Koreans in 2013 and 2014. In 2012, the Constitutional Court stopped websites from registering commenters’ national ID numbers, freeing internet users to interact more anonymously. Yet this positive decision came too late for many. Cyberattacks and online theft have exposed millions of South Korean’s personal details in the past five years, but courts have refused citizens permission to obtain new, uncompromised ID numbers. Moreover, domestic service providers legally cooperate with law enforcement agencies seeking user data even without a warrant, introducing scope for abuse. In December 2013, police accessed private social network accounts and real time location information while seeking to question leaders of a railway union protest.6

---

1 Park’s predecessor Lee Myung-bak, who governed from February 2008 to February 2013, was also in the Saenuri Party, which was known as the Grand National Party until it changed its name and logo in February 2012.
South Korea

The Constitutional Court also reinterpreted election laws in 2011 to allow online campaigning throughout the year; it was formerly restricted during campaign season. This welcome step was followed by a flood of alleged political manipulation by military and intelligence agents online, resulting in more than a million posts supporting President Park in 2012.

Yet even while individuals responsible for those apparent irregularities faced trial, conservative lawmakers proposed making mobile surveillance technology a legal requirement for telecommunications companies, to improve national security and intelligence gathering. Another proposal would criminalize social media rumors during disasters. It was made after an April 2014 ferry disaster that caused hundreds of unnecessary deaths provoked widespread criticism of the official response. News reports said officials tried to play down the outrage by steering journalists and online comments towards a more positive interpretation, and even sought to investigate teachers whose posts on a government website called for President Park to take responsibility.

Obstacles to Access

South Korea is one of the most wired countries in the world, for both usage and connection speed. Internet penetration was at 85 percent in 2013. 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 ($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 111 percent in 2013—a sign that many users now have more than one device. Moreover, smartphone users represented 75 percent of all mobile subscribers as of November 2013. Wi-Fi coverage has increased rapidly to accommodate smartphones and tablet com-

7 Before this ruling, the National Election Commission applied 93(1) of the Public Official Election Act, which bans the display and distribution of election-related paraphernalia for 180 days before the polls, both offline and online alike, with penalties of up to 2 years’ imprisonment or a fine of up to KRW 4 million (US$3,636). See: Yeon-Ok Lee & Han Woo Park, “E-Campaigning Versus the Public Official Election Act in South Korea: Causes, Consequences and Implications of Cyber-Exile,” Aslib Proceedings 65(4), 2013, 388-405.
13 Sutter, “Why Internet connections are fastest in South Korea.”
14 International Telecommunication Union, “Mobile-Cellular Telephone Subscriptions, 2000-2013.”
computers. Free Wi-Fi is offered in over 1,000 public spaces across the country, including train stations, airports, libraries, national public hospitals, community centers, and select tourist spots.\textsuperscript{16}

Omnipresent and affordable cybercafes have helped prevent a digital divide in South Korea. Known as PC bang (room), many offer broadband access for approximately $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.\textsuperscript{17}

The telecommunications sector in South Korea is relatively diverse and open to competition, with 119 internet service providers (ISPs) operating as of December 2013.\textsuperscript{18} Nevertheless, it is dominated by three companies: Korea Telecom (44 percent), SK Telecom (24 percent), and LG Telecom (15 percent). The same firms control equivalent shares of the country’s mobile service market, at 31.5 percent, 50 percent, and 18.5 percent respectively.\textsuperscript{19} All three companies are publicly traded (Korea Telecom was state-owned until privatization in 2002), but they are part of the country’s chaebol—large, family-controlled conglomerates connected to the political elite, often by marriage ties.\textsuperscript{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.\textsuperscript{21} Korea Mobile Internet (KMI), a consortium of mobile virtual network operators who rent capacity from the main players, was making a sixth attempt to enter the market in May 2014. In July, outside the coverage period of this report, the Ministry of Science, ICT and Future Planning rejected their bid for a license for failing to meet financial requirements, which a KMI spokesman described as “excessively strict.”\textsuperscript{22}

The conservative Lee Myung-bak government, which was in power from February 2008 to February 2013, restructured regulatory institutions dealing with ICTs. 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.\textsuperscript{23} The KCC consists of five commissioners, with the president appointing two (including the chairman) and the National 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.\textsuperscript{24} 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 ($545,000) for influence peddling. Lee pardoned him at the end of his term in January 2013.

In March 2013, President Park Geun-hye missed an opportunity to distance herself from this history of cronyism, naming her close aide and former 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.

**Limits on Content**

_The head of national intelligence was on trial during the period covered in this report for allegedly orchestrating millions of tweets and online comments in support of President Park before the December 2012 election. The Ministry of Defense said officials in the ministry’s cyber unit posted inappropriate political content during the same period. Directives were also found to be circulated to contain the spreading of social media content that criticized the Park Geun-hye administration after a ferry disaster in April 2014. Thousands of websites continued to be blocked or deleted, some for content related to North Korea. Internet users protested, and considered a legal challenge, when the copyright commission blocked music-streaming and torrent-sharing sites without notifying service providers._

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. According to official figures, 85,644 websites or pages were censored in 2013, 62,658 blocked and 22,986 deleted.

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 the 1948 National Security Act, which bans content that “praises, promotes, and glorifies North Korea.” Police reported that 27 foreign sites, 338 social networking accounts, and 132 online communities were blocked and 15,168 items of propaganda were deleted for jeopardizing national security in 2013.

Censorship is predominantly carried out on the orders of the Korea Communications Standards Commission (KCSC), which was established in 2008 to maintain ethical standards in broadcasting.

---

26 BBC, “South Korean president issues controversial pardons,” _BBC News_, January 29, 2013, [http://bbc.in/3Ce70](http://bbc.in/3Ce70).
28 Among those blocked, 28,894 were for “encouraging gambling,” 17,608 for “prostitution and obscenity,” 12,759 for “illegitimate food and medicine,” 1,745 for “violating others’ rights,” and 1,652 for “violating other laws and regulations.” Among those deleted, 8,538 were for “illegitimate food and medicine,” 7,527 for “violating other laws and regulations,” 4,767 for “prostitution and obscenity,” 1,388 for “violating others’ rights,” and 766 for “encouraging gambling.” Statistics published quarterly by the Korea Communications Standards Commission at [http://bit.ly/1iDTDoX](http://bit.ly/1iDTDoX) (in Korean).
South Korea

and internet communications. In its first year, 4,731 websites or pages were blocked, and 6,442 deleted; its activities have increased since then. Nominally an independent statutory organization, its nine members are appointed by the president.\(^{32}\)

Observers criticize the body’s vaguely defined standards and wide discretionary power to determine what information should be censored.\(^{33}\) A team of 20 to 30 monitoring officers flag possible offenses, including obscenity, defamation, and threats to national security. The police and other authorities can refer matters to the commission, and individuals can also submit petitions. Commissioners meet every two weeks to deliberate over flagged cases, and then issue censorship orders to content hosts or service providers.\(^{34}\) Noncompliant service providers face up to two years’ imprisonment, or a fine of up to KRW 10 million ($9,000), under the Comprehensive Measures on Internet Information Protection issued by the KCC in 2008.\(^{35}\)

In 2011, law professor Park Kyung Sin, then one of the KCSC’s nine members, challenged the institution’s criteria by posting an image of human genitalia on his personal blog for public discussion.\(^{36}\) Fellow KCSC members began evaluating his blog for deletion and Park subsequently took the pictures down, but prosecutors fined him KRW 3 million ($2,700) in 2012 for violating obscenity laws.\(^{37}\) A higher court in Seoul cleared him on appeal,\(^{38}\) and the Supreme Court is hearing a challenge by the prosecution. Park’s blog is still available.\(^{39}\)

A major cause for concern is that authors of blocked or deleted content are never notified of the commission’s decision, nor given an opportunity to defend their right to publish.\(^{40}\) While KCSC meeting minutes are available online,\(^{41}\) and content owners can challenge the commission’s ruling, there is no independent avenue for appeal. This allows the KCSC to make politically, socially, and culturally biased judgments, often lacking legal grounds. In many cases, the KCSC blocks entire blogs even though only a small portion of posts are considered to be problematic.

---

\(^{31}\) 3,816 websites or pages were blocked for “encouraging gambling,” 549 for “disturbing social order,” and 366 for “obscenity”; 2,238 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.”

\(^{32}\) 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/1aYv0GA.


\(^{34}\) Author’s interview with Park Kyung Sin, who served as a commissioner until his resignation in 2014, at the KCSC office, April 4, 2013.


\(^{39}\) K.S. Park’s Writings (blog). http://blog.naver.com/kyungsinpark.

\(^{40}\) Interview with Kyung Sin Park.

\(^{41}\) Available at http://bit.ly/1djdju1 (in Korean).
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. Since 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 5 percent of the total considered by the KCSC, according to Park Kyung Sin.

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 remove it. On receiving a request, the company must hide the content for 30 days. Content is permanently deleted if its owner does not revise it or appeal within 30 days. 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.

International companies offering online maps are restricted from exporting South Korean map data to servers overseas under a wartime law to guard the country’s geographic information from North Korea. In September 2013, the Land Ministry said it would allow foreign companies to use an English-language digital map on a case-by-case basis, but would not allow Google or other map providers to enhance or process the map on servers outside the country, in order to provide navigation or other services.

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 Korean Copyright Commission, to shut down an entire bulletin board 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 November 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 activists and some users of the site plan to challenge the order in a lawsuit.
In South Korea, restrictions on political speech surrounding elections are more stringent than in many democracies due to limits prescribed in the 1994 Public Official Election Act. The National Election Commission applied the same limits online, resulting in content deletion and fines, until the Constitutional Court ruled the law could not be interpreted to restrict digital campaigns in 2011.51

In December 2012, opposition lawmakers accused a National Intelligence Service (NIS) agent of manipulating 40 different online accounts to discredit opponents of then-presidential election candidate Park Geun-hye. Police cleared the agent in an unusual late-night announcement three days before the polls, which a junior prosecutor later described as a cover-up.52 In June 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 the political opposition as sympathizers of North Korea.53 Park Geun-hye denies ordering or benefiting from digital manipulation.54 Won and his successor, Nam Jae-joon, admit they refuted North Korean propaganda in online forums but deny political motives.55 In late 2014, Won was given a suspended sentence under a law which bars intelligence officials from political activity, but acquitted of trying to sway the election.56 In December 2013, the Defense Ministry’s cyber command unit, launched in 2010 to “combat psychological warfare in cyberspace against North Korea,” 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.57

Attempts to manipulate content were evident again in April 2013 following a ferry disaster which cast the government in a poor light. An investigation subsequently revealed the vessel was operating illegally after being decommissioned, and that the 300 casualties—mostly high school students—died during an incompetent rescue operation when passengers were directed to their cabins while the ship slowly sank. 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.58 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 the news report. The Ministry of Oceans and Fisheries separately issued a similar directive. In May conservative legislator

51 Lee & Park, “E-Campaigning Versus the Public Official Election Act in South Korea.”
55 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.
South Korea

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 ($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, he said that KCSC censorship discourages government criticism, limiting the public’s ability to ensure oversight and accountability.

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. Born out of this was a variety of alternative and activist media outlets on the internet. The most thriving example is 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 a December 2013 report, warning their owners not to report on issues outside their remit. How this vague caution might affect the outlets named is not clear, but observers interpreted it as a signal that authorities may seek to regulate online news.

South Koreans have embraced online technology for civic engagement and political mobilization. Filmmakers have successfully solicited funding via social media for socially conscious films, such as “Another Promise,” which documents poor working conditions in Samsung semiconductor factories. The film topped the box office in the first week of its release in February 2014, despite main cinema franchises refusing to screen it. Ironically, the most striking example of digital mobilization of the coverage period used traditional, offline tools when students sparked a nationwide trend of expressing grievances on public, handwritten posters. The movement went viral after it was documented on the internet.

---

59 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), Mediaus, May 2, 2014, http://bit.ly/1sZO1mj.
60 Available at http://blog.naver.com/kyungsipark/110190423160.
65 Yoo Eun Lee, “South Korean Authorities Discredit Dissenting Voices.”
Violations of User Rights

While Park Geun-hye denied manipulating online content for political benefit, civil and criminal cases against her online critics spiked. Disproportionate penalties included an 18-month prison sentence for defamation in November 2013, while prosecutors explored increasing sanctions for defamation committed online. Courts also made positive rulings. In August 2013, two years after police detained Twitter user Park Jung-geun for sharing content from North Korea as a joke, a court cleared him of a 2012 conviction under Article 7 of the National Security Act. Yet social media providers continue to cooperate with law enforcement without judicial oversight. In December 2013, police sought leaders of a Korean Railway Workers’ Union protest using personal details from their online accounts obtained without warrants. Meanwhile, conservative lawmakers proposed mandating that telecommunications companies incorporate mobile surveillance technology to facilitate intelligence gathering. While specifics remain murky, the proposal came at a time when many South Koreans are questioning their lack of digital privacy protections. In the wake of cyberattacks that exposed millions of personal ID numbers and credit card details, the Constitutional Court is hearing an appeal by citizens whose suit to change their compromised IDs was denied by lower courts.

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 internet users for online activities has generated a chilling effect and international criticism.68

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,69 and that any visit to websites or pages maintained by people of North Korea must be reported to the government in advance.70 Anyone failing to do so faces a fine of up to KRW 1 million ($900).

National security prosecutions against individuals expressing North Korean sympathies have increased under conservative rule. Cases involving online communication rose from 5 in 2008 to 82 in 2010, a trend which looks set to continue.71 Overall, national security arrests increased 19 percent and detentions 37.5 percent, in the first year of the Park Geun-hye administration.72 Film director

68 La Rue, “Full Text of Press Statement.”
70 Reports of such contact, online and offline, are to be made through an online system at http://www.tongtong.go.kr/.
Shim Seung-bo, for example, was given a suspended sentence of 10 months in prison in February 2014 for running a pro-North online forum.  

In August 2013 a higher court cleared photographer Park Jung-geun of a 2012 conviction for retweeting posts from a North Korean Twitter account. He said the retweets were intended to make fun of the regime, but police raided his studio in September 2011 and jailed him for one month in January 2012 before releasing him on bail. A court had sentenced him to a suspended 10-month prison term for “supporting ... anti-state activity” in November 2012.

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 ($9,000), regardless of the truth of the contested statement. Insults, which unlike defamation offenses must be instigated directly by a complainant, are punishable by a maximum KRW 2 million ($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 ($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. In August 2013, the Supreme Prosecutors’ Office announced in a directive to lower offices that it would enhance sanctions against online defamation.

While the directive is nonbinding and its consequences may be difficult to pinpoint, digital defamation cases involving criticism of politicians and public figures are increasing. In April 2013, former Gyeonggi provincial police chief Lee Cheol-gyu sued 55 Twitter users for sharing a document listing him among public officials who allegedly accepted sexual bribes. In a summary indictment, 27 out of the 55 users were fined between KRW 300,000 and 3,000,000 ($270 to $2,700) in January 2014, though many demanded a formal trial instead.

Numerous online defamation cases involved President Park Geun-hye. In February 2013, the month Park took office, a court in Incheon fined a citizen KRW 800,000 ($720) for making libelous statements against Park in the comments section of a news website six times during 2012. Another citizen, Huh, in Uijeongbu in Gyeonggi province was given a one-year suspended jail sentence in August 2013 for 114 defamatory posts against Park on the conservative daily Chosun Ilbo’s website.

---

South Korea

including one calling her a “dictator’s daughter.” In October, 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. The following month, a judge in southern Jeonju city convicted poet Ahn Do-hyun and gave him a suspended fine of KRW 1 million ($900) for repeating 17 times on his Twitter account that Park was in possession of property stolen from a famous anti-Japanese colonial fighter. The jury, which provides judges with influential but nonbinding judgment recommendations in South Korea, had found him innocent, which may account for the non-collection of the fine. Ahn was cleared in a March 2014 appeal.

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. 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 August 2012, the Constitutional Court ruled Article 44(5) unconstitutional, citing privacy vulnerabilities from cyberattacks among other factors. 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, but the incident renewed public concern about internet users’ right to privacy. Fifteen citizens filed a lawsuit to be able to change their RRNs, but the Seoul Administrative Court and the Seoul High Court ruled against them. The case is currently in the Constitutional Court.

The Personal Information Protection Act was amended in August 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 will be punishable by fines of up to KRW 500 million ($455,000). Mobile service providers still require users to provide their RRNs.

---

85 The amendment became Article 82, Provision 6.
South Korea

Other laws, such as the Public Official Election Act, the Game Industry Promotion Act, and the Telecommunications Business Act, separately require internet users to verify their identities. To ensure compliance with these laws, the KCC is exploring registration options beyond RRNs, such as Internet Personal Identification Numbers (i-PINs), authenticated certificates (issued by banks and other organizations permitted to collect RRNs by Article 23 of the Network Act), and SMS verification. Notably, a Children and Youth Protection Act amendment increased the scope of content that requires identity verification in 2012, stating the goal was to better protect young people online (RRNs contain digits from the user’s birth date that show their age). Violations of the act rose from 100 in 2011 to 2,224 in 2012, according to a report published by the Supreme Prosecutors’ Office, and many offenders ended up with disproportionate penalties.

In April 2013, conservative lawmaker Shin Eui-jin proposed a new bill to classify “online games and other digital media content” as addictive, along with alcohol, narcotics and gambling, and subject them to tougher government controls. The bill remained under consideration in May 2014.

Service providers “may” surrender individuals’ personal information without a warrant to investigative agencies, including police, prosecutors, and the National Intelligence Service, under Article 83(3) of the Telecommunications Business Act, but the clause is non-binding. In 2012, in a KRW 20 million ($18,000) suit by a user against a major web portal service who provided personal data 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 ($460) in compensation.

The ruling does not appear to have strengthened privacy safeguards. According to the latest official press release in October 2013, service providers fulfilled 465,304 such requests in the first half of 2013, a 17.8 percent increase over the number they executed during the same period in 2012. During a union protest against the government’s rail privatization plans in December 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. During 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...”

93 Personal information 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.
94 Kang, “Portal sites that neglected malicious comments liable for defamation.”
do not know how much of our personal information was exposed,” a union representative told the media.97

The April 2014 ferry disaster also prompted accusations of privacy violations. The coast guard became subject to public criticism for looking at content on victims’ mobile phones and allegedly tampering with the memory chips before returning them to families.98 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.99

In January 2014, lawmaker Seo Sang-ki proposed what reporters described as “another Big Brother law,” a legal amendment to the Protection of Communications Secrets Act obliging mobile service carriers to install a tapping system within two years or pay a financial penalty up to KRW 2 billion ($1.8 million). Some providers already install this technology on a voluntary basis under the existing act, which requires officials to seek a court order for wiretaps (with exceptions for emergencies) and inform subjects after investigations are concluded. Seo said the amendment would help the NIS curb anti-state activity.100

There have been no reports of physical violence against online users. Technical crimes are more common. A notable increase in technical disruptions in the past three years has highlighted vulnerabilities in the country’s ICT infrastructure. Reported violations of electronic data tripled between 2010 and 2013 from 54,832 incidents to 177,736, according to official figures.101 Recent targets include three major South Korean banks and the country’s two largest broadcasters in March 2013.102 North Korean authorities have been implicated in computer network attacks “targeting critical infrastructure” in South Korea, according to local and U.S.-based research.103 Whether politically or financially motivated, such incidents affect a critical proportion of the population, yet ordinary users are barely protected or compensated.104

In January 2014, a computer contractor working for a credit bureau stole unencrypted personal data, including RRNs and credit card details, belonging to 20 million South Koreans.105 Given the extent of

this exposure, authorities announced that they would revisit the current national ID numbering system, although they made it clear that the RRN itself would be not be abolished.\textsuperscript{106}

Sri Lanka

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></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>20</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>23</td>
<td>23</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>58</td>
<td>58</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 20.5 million
Internet Penetration 2013: 22 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- In March 2014, the information ministry formed a committee to regulate social media, shortly after President Rajapaksa dubbed them a “disease;” the scope of its activities remains unclear (see Limits on Content).

- The Colombo Telegraph website was repeatedly inaccessible, continuing a trend of pressure on online news outlets (see Limits on Content).

- Incidents of violence and harassment against internet users declined, though traditional journalists met with increased intimidation (see Violations of User Rights).
Introduction

International and local journalists met with increased harassment in Sri Lanka in the past year, a trend reflected online when the website of the outspoken Colombo Telegraph newspaper was apparently censored, though the government denied responsibility. Top leaders made ominous statements about social networks threatening national security, suggesting that their policy of regulating and punishing online dissent remains unchanged. However, rights violations targeting internet users—whether attacks, prosecutions or cyber-harassment—declined during the coverage period in comparison with previous reports.

Since coming into power in 2005, the ruling United People's Freedom Alliance (UPFA) has pursued an ambitious ICT policy to improve internet access and digital literacy. However, civil conflict with the Liberation Tigers of Tamil Eelam (LTTE)—which ended in 2009—hindered investment in the information and communication technology (ICT) sector and expansion of the internet across the country. In January 2007, the government made its first attempt to clamp down on internet freedom in response to reportage on the military campaign against the LTTE and civilian casualties.

Content restrictions targeting criticism of the government, including Tamil-language websites, continue. Independent-minded online journalists have also met with violence and extralegal intimidation. In 2014, at least one journalist had been missing since 2010, when colleagues believe he was abducted by government agents. In the context of this repressive record, local and international rights groups criticized the choice of the capital, Colombo, as the location for the Commonwealth Heads of Government meeting in November 2013.

Obstacles to Access

Nearly 22 percent of the population had internet access in 2013, as a continually expanding economic sector and growing youth population drove demand for online services. Government expenditure and private investment in ICTs have resulted in several projects to develop an island-wide telecommunications infrastructure. In 2011, the Telecommunications Regulatory Commission (TRC) announced plans to establish Wi-Fi in schools, government buildings, and public transport areas.

---

As of mid-2014, some private firms report operating over 2,000 Wi-Fi hotspots around the country, suggesting coverage has increased considerably over the last two years.\(^7\)

Internet connectivity became more affordable over the same period with the cheapest broadband connections priced at just under US$5 a month. Internet service providers (ISPs) lowered monthly rates in 2011.\(^8\) In January 2013, telecom operators welcomed a move by the TRC to reduce a tax on broadband internet access by 50 percent.\(^9\)

The majority state-owned ISP Sri Lanka Telecom (SLT) commands more than 50 percent of the market and has the largest fiber-optic national backbone.\(^10\) 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 backbone network.\(^11\)

Increasingly affordable handsets and data packages have boosted mobile internet use, particularly among young people.\(^12\) Monthly subscriptions can run as low as $3 a month. Sri Lanka’s mobile penetration was nearly 99 percent as of September 2013.\(^13\) With over 7.5 million subscribers,\(^14\) Dialog Axiata is the largest mobile service provider, followed by Mobitel (5 million), Etisalat (4.5 million),\(^15\) and Airtel-Bharti Lanka and Hutchison Telecommunications (1 million each).\(^16\) So far, only Dialog Axiata, Mobitel, and Sri Lanka Telecom offer 4G LTE broadband services.\(^17,18\)

Low digital literacy represents a major barrier to ICT use. Although Sri Lanka’s literacy rate is approximately 91 percent,\(^19\) only 20 percent of the population was comfortable using computers in 2009, the last available survey.\(^20\) 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

---

Sri Lanka 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.

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, then center of the conflict with the LTTE, and still a militarized zone. The war also caused severe lags in infrastructure development for the northern and eastern provinces. Since its 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. More positively, preliminary census data published in December 2013 identified heavy internet usage in postwar minority districts in 2011 and 2012, citing Vavuniya in the Northern Province as the district with the country’s highest household internet usage.

As a national regulatory body, the TRC’s actions lack transparency and independence. Under a constitutional amendment ratified in 2011—which also removed presidential term limits—the president can appoint the heads and members of all commissions, subverting legislative guarantees for the independence of the TRC and other statutory institutions. Rajapaksa cemented control of the TRC by appointing his permanent secretary as its chairman. The TRC’s interventions to restrict online content and pronouncements on strengthening online regulation have been partisan, extralegal, and repressive.

### Limits on Content

Targeted, politicized censorship continued throughout 2013 and 2014 with the website of the Colombo Telegraph periodically blocked, apparently because of its dissenting content and coverage of controversial political affairs in the country. As in the past, the government denied responsibility. Hate speech online, however, appeared to subside over the last year, though violent anti-Muslim incidents contin--
ued to be the topic of much discussion on social media, with messages of support extended towards the Muslim community from Facebook users within the country.

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. Implementation is not properly coordinated or comprehensive, with some targeted websites available at times on one or more ISPs and at other times completely inaccessible. Officials cite ill-defined national security measures to legitimize these measures, though websites have been blacklisted for content related to human rights issues, government accountability, corruption, and political violence. Censors have targeted the political opposition and independent news, including Tamil websites, sites run by Sri Lankans in exile, and citizen journalism platforms, though usually without acknowledging a political motive. The government also restricts access to pornography.

Officials monitor websites for sensitive political content and direct the TRC to blacklist them, which in turn requests ISPs to block access. 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. 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 its requests or sought judicial oversight.

Blocking has continued at low but consistent levels in recent years, including at least three Tamil-language news websites censored in 2012. The exile-run news website TamilNet has been blocked since 2007 for its support of Tamil rebels. The Colombo Telegraph website has been periodically blocked since it first started reporting on political issues in the country, though authorities denied responsibility in August 2013. In March 2014, the website was blocked once again, and remained inaccessible despite the concern expressed by opposition parties. In May 2014, two more websites, the Sri Lanka Mirror and the Independent, were blocked allegedly for publishing news items that were critical of the government.

It is not clear whether the government has resources to implement deep-packet inspection (DPI) that would enable real-time filtering and other, more sophisticated censorship methods. In 2010, local news reports said IT military intelligence experts from China—where such methods are well-established—were assisting the government in blocking “offensive” websites. In 2014, the New York Times reported that the Sri Lankan government “has hired a Chinese company” to censor online news, but did not report more details. Despite anecdotal reports that some Sri Lankan telecoms have DPI capabilities to enhance mobile data services, there is no evidence to date that these have been used to censor content.

In 2011, the government announced plans to introduce more comprehensive legislation to control internet use, ostensibly to crackdown on child abuse online. However, regulations introduced since then target independent news and opinion, including the Ministry of Mass Media and Information’s 2011 registration policy for websites carrying ill-defined “content relating to Sri Lanka or the people of Sri Lanka,” a move unsupported by law which could potentially be used to hold owners responsible for information posted by users. Local news outlets reported in 2012 that the ministry had rejected over 50 registrations due to “false and incomplete” registration details, though how they assessed the veracity and which websites were affected remains unclear. Also in 2012, the defense ministry’s Media Centre for National Security directed news organizations to submit SMS news alerts containing content related to “national security and security forces” for prior approval, shortly after coverage of the killing of three soldiers in the northern province. The center did not outline a legal basis for the directive; SMS news alerts continue to be disseminated by news operators, but with a noticeable lack of coverage of military issues.

In 2012, the media ministry directed the cabinet to amend the notorious Press Council Act No.5 of 1973, making news websites subject to the same draconian content regulation as traditional 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 had lain 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 extending the restrictions to digital media. The amendment instituted a hefty registration fee of LKR 100,000 ($790), plus an annual renewal fee of LKR 50,000 ($395), costs which

---

threaten to inhibit the emergence of new websites and force existing ones out of operation. It failed to define what constitutes “news,” providing leeway for authorities to scrutinize a wider range of online platforms like blogs or social media.

The trend continued in June 2013 when the ministry proposed a new code of ethics for print and electronic media. The code contained broad provisions prohibiting the publication of thirteen types of speech, including content that “offends against expectations of the public, morality of the country,” content that “contains material against the integrity of executive, legislative and judiciary,” and content that “contains criticism affecting foreign relations.” When questioned about the necessity of the code, Minister of Mass Media and Information Keheliya Rambukwella said, “Well, at some point we need to start regulating the media.” Following opposition by free speech activists and condemnation by international rights groups, the government appears to have set the code aside.

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. In December 2011, one settled out of court, agreeing to several TRC conditions—such as removing links to blocked content—in return for restored access.

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, 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. 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.

---


54 At least one of these sites – [www.lankaenews.com](http://www.lankaenews.com) - continues to be periodically blocked in the country.


The government actively encourages self-censorship “on matters that would damage the integrity of the island,” and many mainstream news websites comply, 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 support the UPFA government. These and official government websites have waged smear campaigns against government critics in the past.

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. Many of the relevant social media pages have since been removed, and the activity declined during the coverage period of this report, though without stopping altogether.

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. However, the networks came in for high-level criticism. In June 2013, Gotabhaya Rajapaksa called social media a threat to national security, providing a platform for “propagating certain ideologies online and mobilizing and organizing people.” This view was reinforced by President Rajapaksa in October when he stated that social media sites like Facebook are a “disease” and that there are “ways” to block them, though he himself maintains an active Facebook page and Twitter profile. In March 2014, the information ministry announced that it had formed a committee to look into regulating social media in order to “control the spread of information without credibility as well as to prevent its misuse and criminal activities connected to the Internet.” While the stated intent of the committee was to address cyber-harassment, it caused concern among digital activists. In May 2014, President Rajapaksa reaffirmed his intent to regulate

---

61 Haviland, “The Hardline Buddhists Targeting Sri Lanka’s Muslims.”
64 Social media is a threat to national security says Gotabhaya Rajapaksa in speech delivered to Defence University,” The Republic Square, June 14, 2013, http://www.therespublicsquare.com/politics/2013/06/14/social-media-threat-national-security-gotabaya/
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."\(^{67}\)

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. Some previously blocked content was available in 2014. Citizen media site *Groundviews* and its sister site *Vikalpa* were also operating freely, despite SLT temporarily blocking them for a day in 2011.\(^{68}\) The platforms report on topics that would otherwise not be covered by the mainstream media and provide links to circumvention tools.\(^{69}\) Another website, *The Republic Square*, started up in mid-2013 and has become a widely read news platform. Although online content by Human Rights Watch and Transparency International has been blocked in the past when the groups criticized the Rajapaksa administration,\(^{70}\) websites belonging to international media and human rights groups were freely accessible in 2014.

**Violations of User Rights**

_During the coverage period, foreign journalists were detained and at least one web journalist remained missing for the fourth year. Fewer rights violations affecting internet users were reported, and physical attacks and threats against journalists, including many linked to government actors, have decreased since the war and its immediate aftermath. But the failure to investigate past incidents cast a long shadow, perpetuating fear and self-censorship._

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.\(^{71}\) 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.\(^{72}\) 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.\(^{73}\)

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 rights 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.\(^{74}\) 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.”\(^{75}\) As of mid-2014, the ministry had made no announcements regarding the legislation’s implementation.

As in past years, the government obstructed 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 President Rajapaksa in May 2010—recommended RTI legislation as a necessary step towards addressing past and ongoing rights violations.\(^{76}\) UPFA parliamentarians rejected an opposition-backed bill in 2011,\(^{77}\) and in 2012, Charitha Herath, the media ministry secretary, said national security concerns would continue to delay the bill, which had yet to be presented in mid-2014.\(^{78}\)

In mid-2012, police arrested nine staff from two news websites. Criminal Investigations Department (CID) officials raided the offices of the *Sri Lanka Mirror* and *Sri Lanka X News* in June on grounds of “propagating false and unethical news on Sri Lanka.”\(^{79}\) The action had scant foundation in law. The CID obtained a search warrant and arrested the employees citing violation of Articles 115, 118 and 120 of Sri Lanka’s penal code. Articles 118 and 120 broadly deal with defamation and the incitement of contempt and hatred, although Article 118 was repealed in 2002, and Article 115 covers conspiracy to overthrow government by coercion.\(^{80}\) 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\(^{81}\)—failure to register the website, ridiculing the president, and evidence of an attempt-

---


ed 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, violation of their right to free expression, and their profession. Hearings are ongoing. Media activists, rights organizations, and diplomatic missions viewed the arrests as intimidation stemming from the websites’ pro-opposition reporting. External Affairs Minister G.L Peiris’ defense of the raid compounded that view when he accused the sites of turning “deaf ears to repeated warnings to tone down their coverage.”

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.”

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, 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 writing anonymously. Digital activists in Sri Lanka also believe Chinese telecoms ZTE and Huawei, who continue to collaborate with the government in the development and maintenance of Sri Lanka’s ICT infrastructure, may have inserted backdoor espionage and surveillance capabilities.

---

There were no new reports of arrests made for information shared by email or text message. Sri Lankan police have made such arrests in the past, though whether the content was obtained through extrajudicial surveillance is not clear. Following the 2010 presidential election, a Media Centre for National Security spokesman told local journalists that police had detained “a few people” for text messages criticizing the outcome of the polls, without elaborating.\(^{90}\) News reports said the detainees had disseminated similar content on Facebook and Twitter. The TRC denied tracing critical commentators through social media, and an unnamed source in the telecommunications industry told Sri Lanka’s \textit{Sunday Times} the police could have been acting on complaints from message recipients.

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.\(^{91}\) Real-name subscriptions are already normal procedure, but the call for registration in 2010 required further information, including photo identification and up-to-date residential details. Unregistered users risk disconnection if they failed to comply, though no cases have been reported.

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 \textit{TamilNet} co-founder Dharmeratnam Sivaram, who was found dead in a high-security area outside parliament.\(^{92}\) 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 continues amid a culture of impunity. In August 2013, unidentified assailants attacked an editor of the \textit{Sunday Leader} in her home.\(^{93}\) Frederica Jansz, previously the editor of the \textit{Sunday Leader}, fled Sri Lanka in 2012 after Gotabhaya Rajapaksa threatened her during a telephone conversation.\(^{94}\)

International news reports and rights groups say government soldiers are responsible for the notorious “white van” abductions of critics and activists\(^{95}\)—named after the vehicle often used to carry them out—a claim the administration denies.\(^{96}\) \textit{Lanka-E-News} journalist and cartoonist Prageeth Eknaligoda has been missing since January 24, 2010, after the website backed the political opposition in elections.\(^{97}\) Officials say he sought asylum overseas.\(^{98}\) The inaction on his case, combined with other methods of intimidation including arson attacks and legal harassment, forced \textit{Lanka-E-News}

\(^{90}\) “Monitoring Cyberspace to Regulate Anti-Govt. Content,” February 14, 2010, \url{http://sundaytimes.lk/100214/News/nws_50.html}.
\(^{93}\) “Critical Sri Lankan newspaper editor held at knife point,” CPI, August 26, 2013, \url{http://cpj.org/2013/08/critical-sri-lankan-newspaper-editor-held-at-knife.php}.
\(^{95}\) “A Disappearance Every Five Days in Post-War Sri Lanka,” \textit{Groundviews}, August 30, 2012, \url{http://groundviews.org/2012/08/30/a-disappearance-every-five-days-in-post-war-sri-lanka/}.
and its editor out of the country.\textsuperscript{99} While international journalists faced increased harassment,\textsuperscript{100} there were no attacks on online journalists or internet users during the coverage period of this report.

Cybercrime is a growing problem in Sri Lanka, with illegal breaches of social media and email accounts becoming more common.\textsuperscript{101} Networks associated with the LTTE have been reported attempting to hack into national security networks and carry out web defacement attacks.\textsuperscript{102} The government has recognized the need to strengthen its defensive capability, yet critics fear technology bought for this purpose could be used to restrict legitimate expression.\textsuperscript{103} Cyberattacks have also targeted government critics in the past, though no incidents were reported during the coverage period. The attackers are thought to align with the government. In June 2007, Media Minister Keheliya Rambukwella told journalists “We are looking for hackers to disable... \textit{TamilNet} but could not find anyone yet.”\textsuperscript{104}

\textsuperscript{103} Centre for Policy Alternatives, \textit{Freedom of Expression on the Internet} (2011), 42.
# Sudan

## Internet Freedom Status

<table>
<thead>
<tr>
<th>Obstacles to Access (0-25)</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Free</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>19</td>
<td>19</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>63</td>
<td>65</td>
</tr>
</tbody>
</table>

*0=most free, 100=least free

## Key Developments: May 2013 – May 2014

- A localized internet service disruption in June and a nationwide blackout in September corresponded with large antigovernment protests; the blackouts were reportedly directed by the government (see **Obstacles to Access**).

- U.S. sanctions on Sudan had a negative impact on the ability of Sudan’s civil society to leverage online technologies, inhibiting important civil society efforts (see **Limits on Content**).

- Monitoring and filtering devices from Blue Coat Systems were traced to three networks inside Sudan in June (see **Violations of User Rights**).

- Government surveillance of online activists and journalists was particularly pronounced during the June and September 2013 protests (see **Violations of User Rights**).

- A number of individuals were arrested for their ICT activities, while journalists and civil society groups were subject to an increasing degree of technical violence (see **Violations of User Rights**).
**Introduction**

During the coverage period, journalists, civil society, and citizens at large in Sudan faced an ongoing government crackdown on free expression, triggered by mass protests that took place in June 2013 and smaller demonstrations that ensued through September 2013. The protests were sparked by the removal of government fuel subsidies, which escalated the cost of transportation and food items in a country already suffering from a severe economic crisis.

The period between the widespread “Sudan Revolts” protests in the summer of 2012 and the protests that took place throughout 2013 saw a tightening of press freedom, sporadic arrests of activists, and the shutdown of major civil society organizations. Government repression intensified toward the end of 2013, with the authorities using live bullets and an extensive arrest campaign to break up the September protests, in addition to shutting down all internet services for nearly 24 hours for the first time in Sudan. Access to Facebook and YouTube platforms was slow for days after the shutdown. A shorter internet blackout was reported on one service provider leading up to the June protests.

Meanwhile, the Sudanese government under President Omar al-Bashir increased its restrictions on internet freedom through various tactics during the coverage period. For example, the national regulator reportedly sought ways to control social media applications such as Facebook and WhatsApp, while government trolls within the National Intelligence and Security Service’s Cyber Jihadist Unit increasingly manipulated the online information landscape. Government surveillance of online activists and journalists was particularly pronounced during the September 2013 protests, and sophisticated surveillance technology from U.S.-based Blue Coat Systems was traced to three devices inside Sudan, including on the networks of the Emirati-owned telecom provider, Canar.

A number of individuals were arrested for their online activities during the year, including the journalist Khalid Ahmed from *Al-Sudani* newspaper, who was arrested in June 2013 by the electronic crimes police for an article he was accused of publishing on an independent news website that criticized the army. Meanwhile, journalists and civil society groups were subject to an increasing degree of harassment, extralegal violence, and hacking attacks. In one incident, government authorities shut down the popular TEDxKhartoum event in May 2013. Numerous online news outlets and individual Facebook pages suffered hacking attacks throughout the year.

**Obstacles to Access**

Access to information and communications technologies (ICTs) in Sudan continued to spread in the past year, with internet penetration growing from 21 percent in 2012 to 23 percent in 2013, according to the International Telecommunication Union (ITU). The number of users, however, could be somewhat higher as internet-enabled mobile phones have become widespread and cheaper in

---

Sudan

recent years. In 2013, 25 percent of the population had access to mobile-broadband services, while mobile phone penetration stood at 73 percent, up from 60 percent in 2012.

Sudan’s telecommunications infrastructure and market are among the most developed and liberalized in the region, which has enabled affordable services. As of mid-2014, a monthly mobile internet subscription cost between SDG 2 to 9 (US$0.35 to $1.50) for 100 MB to 1 GB. In general, all companies offer daily internet for rates that do not exceed SDG 1 for basic access, and as a result of market competition, there are ongoing offers that make it possible to enjoy free or lower cost internet services during certain hours.

Aside from mobile internet, users also access the internet from personal desktops or laptop computers through routers or USB modems that cost between SDG 134 and 250 (US$24 to $44), and monthly fixed-line broadband subscriptions that cost from SDG 26 to 200 (US$5 to $35), depending on the package. Secondhand laptops and computers are widely available, and users can make payments toward a computer in monthly installments. Nevertheless, the number of fixed broadband subscriptions in the country is still very low, with a penetration rate of 0.17 percent in 2013 (up from 0.05 percent in 2012), according to the ITU. Meanwhile, cybercafes, which are concentrated in market areas and popular around universities and dorms, charge between SDG 2 to 5 (US$0.35 to $0.87) per hour, 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. In addition, the country’s relatively low prices for mobile and internet access are still out of reach for the majority of the population in Sudan, where the median annual per-capita income was US$579 in 2013, according to Gallup research.

Meanwhile, comprehensive economic sanctions imposed by the U.S. government against the al-Bashir regime since 1997 have been a significant hindrance to users’ access to various ICTs and new media tools. While the sanctions were amended in 2010 to authorize the export of certain ICTs and boost the free-flow of information, and again in 2013 to allow educational institutions to exchange academic research, the sanctions continued to block access to original software made by American companies, effectively limiting free access to knowledge on the internet. For example, important software such as anti-virus suites, e-document readers, and rich-content multimedia applications

---

3 International Telecommunication Union, “Mobile-Cellular Telephone Subscriptions, 2000-2013.”
5 On the Sudani network. Zain network offers more expensive, but still affordable packages with a 1 SDG internet package per day and a weekly subscription costing 5 SDG while MTN offers daily internet packages costing from 0.60 to 1 SDG.
are blocked and inaccessible for users to download. Additionally, software security updates are unavailable, forcing users to rely on outdated versions that make their computers and devices vulnerable to malware and other technical attacks. Smartphones and tablets are also affected, as online stores where users can download and update applications are completely inaccessible in Sudan. Savvy users have been able to turn to circumvention tools such as proxies and virtual private networks (VPNs) to access these blocked services, but ordinary users likely miss out on these key ICT applications. The problem of sanctions-induced inaccessibility poses a serious security threat to activists and human rights defenders, making them unable to use these technologies in their work and potentially exposing them to state surveillance and censorship.

The U.S. sanctions regime has also stunted Sudan's educational potential, as free online educational websites such as Khan Academy, Google Scholar, and Audacity are blocked to users in the country. In January 2014, the free online education company Coursera announced that it had to restrict access to its courses to students from Cuba, Iran, and Sudan, citing U.S. sanctions that prohibit the export of services from for-profit companies to sanctioned countries.11 Similarly, individuals enrolled in massive open online courses (“MOOCs”) at American educational institutions, such as MITx, reported not receiving certificates of completion after passing online exams.12 The EdX platform announced in February 2014, however, that it had found a solution to the sanctions regulations, enabling them to open its services to all students around the world.13 Coursera also announced in September 2014 that it was granted an Office of Foreign Assets Control (OFAC) license to provide services in Sudan and Cuba.14 Nevertheless, the ongoing restrictions were widely criticized as a violation of the universal right to education and likened to censorship.15

There are four licensed telecommunications operators in Sudan: Zain, MTN, Sudatel, and Canar. 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. 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 foreign entities.16 Only Sudatel and Canar have a direct connection to the international gateway and lease access to the global internet to MTN and Zain.

Fairly strong market competition in Sudan's telecoms sector has enabled the growth of fast internet in the country. Under normal circumstances, the internet operates at advertised speeds of up to 21 Mbps on the Zain network in Khartoum and at 7.2 Mbps in other areas. According to May 2014

---

data from Akamai’s “State of the Internet” report, Sudan’s average connection speed is recorded at 3.2 Mbps (compared to a global average of 3.9 Mbps). In addition, Sudan’s broadband adoption (characterized by connection speeds greater than 4 Mbps) was over 20 percent, while the country’s narrowband adoption (connection speeds below 256 kbps) was under 1 percent.

Despite Sudan’s open and liberalized ICT sector, the government has demonstrated an ability to restrict connectivity and access during particular events, such as the partial internet blackout on the Sudatel network on June 29, 2013 that lasted for nearly eight hours ahead of a planned antigovernment rally. A complete internet blackout occurred three months later on September 25, 2013, when the internet intelligence company Renesys confirmed two separate internet blackouts that were reportedly directed by the government. Beginning at 12:47 UTC on September 25, after three days of intense nationwide protests, Renesys reported that “all Sudanese routed networks were withdrawn from the global routing table,” which was “not caused by a single catastrophic technical failure” and “strongly suggests a coordinated action to remove Sudan from the Internet.” Subscribers of the four service providers (Zain, MTN, Canar, and Sudani) were cut off for nearly 24 hours. Renesys also described the incident as “the largest government-directed Internet blackout since Egypt in January 2011.”

Denying responsibility for the blackouts, the government claimed that a major network problem had caused the internet outage, while the National Telecommunications Corporation (NTC), the national regulator, blamed a fire in the office of the Emirati-owned Canar telecom, which rents access to the global internet network to the other providers. Though unconfirmed, analysts strongly believe the incident was most likely orchestrated by the NTC, the state agency that regulates the ICT sector in Sudan.

Founded in 1996 and housed under the Ministry of Telecommunications, the 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.”

---

19 Renesys Corporation Twitter Feed (@renesys), 4:33PM, June 29, 2013, [https://twitter.com/renesys/status/35106082572736640/photo/1](https://twitter.com/renesys/status/35106082572736640/photo/1).
Limits on Content

No new social, political, or religious websites were blocked during the coverage period, though access to Facebook and YouTube was reportedly very slow or virtually inaccessible to many users during and after the September 2013 wave of protests. Government efforts to manipulate the online information landscape became more concerted and systematic. U.S. sanctions on Sudan had a negative impact on the ability of Sudan’s civil society to leverage online technologies, inhibiting important civil society efforts.

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 percent of blocked material is related to pornography. The NTC’s website also gives users the opportunity to submit requests to either block or unblock websites “that are deemed not containing pornography,” 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 NTC and includes a contact email address at filtering@ntc.gov.sd.

Social media platforms are not blocked in Sudan, though access to Facebook and YouTube was reportedly very slow or virtually inaccessible to many users during and after the September 2013 wave of protests. At times, users were able to access the website through the secure “https” protocol instead of “http.” Meanwhile, since 2008, YouTube and the popular Sudanese forum and news website Sudanese Online have been sporadically blocked for various periods for content perceived as too sensitive by the regime, such as articles on the war in Darfur. The blocks typically range from a few days to a few weeks, and when a website becomes accessible again, it can take some time for content to be fully restored. YouTube was last blocked from September to November 2012 in response to the “Innocence of Muslims” video.

The most recent long-term blocking of websites coincided with the June to July 2012 “Sudan Revolts” protest movement, during which the NTC blocked the online newspapers Sudanese Online, Al-Rakoba, and Hurriyat, the latter two of which are known to be antigovernment. All three outlets were eventually unblocked but at times are still difficult to access.

In response to the growth of online publications that are critical of the ruling party, the Sudanese government has stated intentions to enact legal measures to restrict content regarded as “a threat to national and social security.” According to the ruling party media secretary Yassar Youssef Ibrahim in a July 2013 interview, such “threats” encompass not only religiously immoral content, but also

---

25 “Blocking Or Unblock Websites.”
26 Image of a blocked site: https://docs.google.com/file/d/0B6mqwvplJ6l4eRj3RZo156k/edit.
27 OpenNet Initiative, “Internet Filtering in Sudan.”
29 Hurriyat is based in Kampala, Uganda and its editorial staff is comprised of prominent journalists who left Sudan after enduring numerous court trials for their writings. Al-Rakoba, on the other hand, has a number of anonymous journalists inside Sudan but is managed by a group based in the Gulf region.
opposition publications and political criticism. To combat the perceived threats, the secretary advocated for a law to govern electronic media “that grants authorities the right to block websites when they violate agreed upon limitations.”

In May 2014, the national regulator, the NTC, reportedly began a technical study on social networking applications such as Facebook and WhatsApp in an effort to find ways to control their use in the country, citing concerns that the applications encourage indecent activities that go against Sudan’s customs and traditions. Other reports have alleged that the Ministry of Culture and Information in Khartoum state is looking to use sophisticated technical tools to block social media platforms, though the ministry denied any intent to block websites.

As a result of growing online censorship, some opposition news outlets have moved their servers abroad to avoid blocking. For example, Sudanese Online currently operates from the United States, while Sudan Tribune is based out of France and Al Taghyeer (“Change”) is based in the United Kingdom. This trend may continue if a draft media law with implications for digital news is passed (see “Violations of User Rights”).

Despite increasing instances of internet censorship in recent years, online newspapers in Sudan continue 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 National Intelligence and Security Service (NISS) agents against reporting on certain taboo topics. Restrictions on traditional 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. As such, many print newspapers have begun to circulate censored or banned material on their websites and social media pages, and online news outlets are gaining traction. Most recently, independent journalists successfully launched the electronic newspaper Al-Tareeq (“the road”) in January 2014, and the newspaper Sudan Voices launched its online version in May.

Compared to the highly restrictive space for press freedom 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. Nonetheless, self-censorship is prevalent and may be increasing as the government extends its media crackdown to the internet. During the September 2013 protests, some opposition journalists began publishing anonymously to

---

30 Adam Mohamed Ahmad, “We need a law that governs the electronic media,” The Niles, July 10, 2013, http://www.theniles.org/articles/?id=1938
31 Adam Mohamed Ahmad, “Too many red lines: Pressure on Sudan media freedom increases,” The Niles, July 7, 2013, http://www.theniles.org/articles/?id=1288
33 “Sudan looking into ways to control Facebook and Whatsapp,” Sudan Tribune, May 28, 2014.
35 Interview with an editor-in-chief in Khartoum, Sudan, August 2012.
36 The NISS carries out arbitrary arrests, may detain an individual for up to 45 days without charges and can renew the detention period after the end of the 45-day period. NISS officers have total immunity from the law. “Sudanese Security Service Carries out Brutal Campaign Against Opponents,” Amnesty International, July 19, 2010, http://www.amnesty.org/en/news-and-updates/report/sudanese-security-service-carries-out-brutal-campaign-against-opponents-2010
37 Al-Tareeq: http://www.altareeq.info/ar/
38 Sudan Voices: http://sudanvoices.com/
Government efforts to manipulate the online information landscape have become more concerted and systematic. In response to the Arab Spring events and the proliferation of antigovernment protest movements organized on social media sites in 2011, the Sudanese government began deploying a force known as the Cyber Jihadist Unit tasked to conduct “online defense operations” and “crush online dissent.” A leaked 2011 document revealed that the Unit employs over 200 individuals divided across different locations who work three shifts to ensure around the clock coverage, particularly during timeframes when internet traffic is highest, such as late at night and during the weekend. More recent research from 2013 found that the number of recruits has increased, with the NISS recruiting heavily at government universities, especially at the police-owned Al-Ribat University. The Unit seems to have adequate funding for training, and stipends are given to the young recruits who are mostly students or unemployed youth. According to private interviews, the Cyber Jihadists have also received training courses in hacking and online monitoring from India and Malaysia, among other countries.

Based at the NISS, the Cyber Jihadist Unit proactively monitors content posted on blogs, social media websites, and online newspaper forums. The Unit also infiltrates online discussions in an effort to ascertain information about cyber-dissidents and spread misinformation. This strategy has been employed most prominently on the news forum, Sudanese Online, which is known for its popularity among antigovernment intellectuals, journalists, politicians, and activists. When the government took notice of the website’s influence in the mid-2000s, it planted contributors to spread false information, instigate problems between users, and discredit posts written by members of the forum. The Unit also frequently hacks websites and personal email and social media accounts of activists (see “Violations of User Rights”).

On May 10, 2014, NISS allegedly launched a rumor that it had arrested the administrators of an opposition group’s Facebook page, publishing the story in a print progovernment newspaper (Al Saita) with the headline, “National Security Arrests the Creators of al Bashir’s Diaries.” Created over two years ago, the popular Facebook page is known for its use of humor and satire to criticize the government. Within a day, the administrators announced on their Facebook page that the news

41 Interview with a press freedom advocate and journalist in Khartoum, Sudan, January 16, 2012.
42 Interview with telecommunications expert in Khartoum, Sudan, January 15, 2013.
43 In August 2012, a thread on Sudanese Online titled, “Accounts Targeted and Monitored by the Cyber-Jihad Unit,” started by an exiled activist revealed a list of 274 names, Facebook pages and groups and described the expanded technical capacities of the unit. Leaked to the exiled activist by “a trusted source,” the list made evident that the unit’s primary targets were online activists, particularly young people, whose social media accounts publish timely information about the protests and news about human rights violations. For example, the first name mentioned in the list was Amani Al-Agab, a well-known online activist who is very active on Sudanese forums as well as Facebook. There is little information available on Amani Al-Agab; however, it is known that she is outside Sudan. http://www.change.org/users/7806131; See also, Bukhari Osman, “Accounts Targeted by Cyber Jihad Unit” [in Arabic], August 23, 2012, Sudanese Online, http://www.sudaneseonline.com/cop-bin/sd9b/2bb.cgi?seq=print&board=400&msg=1345716699&rn=1.
article was a rumor, though the false story indicates how the authorities may be trying to crack down on social media by instilling a fear of reprisal among users.

Meanwhile, blogging is an increasingly important platform for journalists and writers who use it 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-2014, there are about 300 Sudanese blogs registered in the newly established Sudanese Bloggers Network. The more active Sudanese bloggers write in the English language.

The internet has also become a powerful tool for activists to fight for social, political, and economic change, enabling protests such as the ones in June and September 2013 to organize across the country. During the damaging floods that befell Khartoum state in July and August 2013, youth activists turned to Facebook to launch the grassroots campaign known as Nafeer to help flood victims. Working with a local NGO, the Nafeer Facebook campaign attracted over 5,000 volunteers within two weeks, in addition to collecting generous cash donations from Sudanese based both locally and abroad, which allowed emergency relief to be delivered to victims more quickly than aid from the government.

Nevertheless, U.S. sanctions have had a negative impact on the ability of Sudan’s civil society to leverage online technologies such as crowd-funding or online payment platforms, which has inhibited important civil society efforts. For example, when Nafeer turned to the internet to seek both volunteers and donations during the August 2013 floods, its Paypal account was shut down for receiving donations from the diaspora in the United States. Similarly, many organizations have been unable to receive financial support from Sudanese diaspora communities that can strengthen their independence from foreign aid as well as their sustainability.

Crisis mappers have also noted that the sanctions are limiting their ability to access the tools they need. According to Abeer Awad Khairy, a crisis mapper who created an online map for the August 2013 floods used by Nafeer and the United Nations to identify regions in need of relief, all Google products are sanctioned in Sudan, including Google Crisis Map and People Finder. Crisis mapping tools produced by other American companies such as Esri, which makes GIS technology for mapping, are also blocked, making it difficult for a proper network of crisis mappers to operate within the country.

Sanctions have further inhibited diaspora communities seeking to send assistance home via crowd-funding tools. In December 2013, for example, a group of Sudanese diaspora activists living

47 Author’s Research.
48 Tweet by @Amjedfarid (in Arabic): “The Americans closed #Nafeer’s paypal account because of sanctions. What are we supposed to deal with, the government’s harassment or the Americans?” August 21, 2013, https://twitter.com/amjedfarid/status/370239060427550720.
in the United States, Europe, and the Middle East launched a crowd-funding campaign via the online platform Indiegogo to help renovate a school in the peripheries of Khartoum that gives free education to 330 internally displaced students from the Nuba Mountains and Darfur.\textsuperscript{50} Within five days of launching the campaign, the group received a message from Indiegogo saying that the campaign had been “frozen” because it may have been in violation of U.S. sanctions policies. In response, the fundraising team attached the most recent OFAC update on Sudan sanctions from November 2013, which provides an exemption for conflict areas and communities impacted by conflict, as well as on the peripheries around Khartoum.\textsuperscript{51} Fortunately, Indiegogo accepted the explanation and put the campaign back online after freezing it for 24 hours.

\section*{Violations of User Rights}

Monitoring and filtering devices from Blue Coat Systems were traced to three networks inside Sudan in June 2013. Government surveillance of online activists and journalists was particularly pronounced during the June and September 2013 protests. A number of individuals were arrested for their ICT activities during the coverage period, while journalists and civil society groups were subject to an increasing degree of technical violence.

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. A permanent constitution is still being drafted as of mid-2014, leaving the INC as the country’s highest binding document.

Sudan has a host of restrictive laws that seeks to limit internet freedom. For example, the Informatic Offences (Combating) Act (known as the IT Crime Act, or electronic crimes law),\textsuperscript{52} criminalizes the establishment of websites that criticize the government or publish defamatory material and content that disturbs public morality or public order.\textsuperscript{53} Violations involve fines and prison sentences between two to five years. While only one case of defamation has been filed under the IT Crime Act since its enactment in 2007,\textsuperscript{54} the act inherently contradicts Sudan’s constitutional protection of freedom of expression and fundamentally undermines internet freedom in the country.

For bloggers and online activists, the press laws and the criminal law are more dangerous. In 2009, the government revised the highly restrictive 2004 Press and Printed Press Materials Law, which continued to allow for restrictions on the press in the interests of national security and public order.

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{50} “Support Nuba Mountain IDP Students,” Indiegogo campaign, December 13, 2013, \url{http://www.indiegogo.com/projects/support-nuba-mountain-idp-students/x/5649009}.
\item \textsuperscript{51} E.O. 13412 exempts Southern Kordofan/Nuba Mountains State, Blue Nile State, Abyei, Darfur, and marginalized areas in and around Khartoum – referred to as “the Specified Areas of Sudan” – from certain of the prohibitions imposed by E.O. 13067. See, Department of the Treasury, “Sudan Sanctions Program,” Office of Foreign Assets Control (OFAC), November 5, 2013, p. 3, \url{http://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf}.
\item \textsuperscript{54} Details of case unknown. Interview with a press freedom advocate in Khartoum, Sudan, January 16, 2012.
\end{enumerate}
\end{footnotesize}
and holds editors-in-chief liable for all content published in their newspapers.\textsuperscript{55} While there is no specific reference to online media, the press law's broad wording allows for its application to online content.

In December 2012, a new draft press law was presented to the national assembly that aims to further restrict media freedom in Sudan. While the draft law has yet to be publicly released as of mid-2014, a member of the Sudanese National Council asserted in an interview with the Doha Centre for Media Freedom in April 2013 that the new law would include regulations on online media.\textsuperscript{56} Meanwhile, the authorities also restrict media freedom through the 2010 National Security Act, which gives the NISS immunity from prosecution and the permission to arrest, detain, and censor newspapers under the pretext of national security.\textsuperscript{57} Furthermore, Sudan's judiciary is not independent, though it has recently ruled against the government in support of press freedom, reversing a government order to shut down the \textit{Al-Tayar} independent daily in March 2014.\textsuperscript{58}

Bloggers and citizen journalists in Sudan are increasingly detained and harassed for their work, particularly during times of protest. In June 2013, national security agents arrested the journalist Khalid Ahmed from \textit{Al-Sudani} newspaper for allegedly publishing an article in an independent news website that criticized the army in Abu-Karshola town in Southern Kordofan, where the government has been at war with the Sudan People's Liberation Movement (SPLM) rebels since June 2011. Despite his claim that he had not written the article, Ahmed was taken to the intellectual property rights court where he was charged with “harming the morale of the Sudanese armed forces,” “sharing military information,” and “tarnishing the reputation of the army's chief of staff” under the penal code and IT Crime Act.\textsuperscript{59} The court cleared Ahmed of all charges in March 2014 due to lack of evidence,\textsuperscript{60} but journalists worry that the incident will set a precedent for the authorities to continue prosecuting online journalists.

In July 2013, three youths were arrested in Northern Kordofan for posting and commenting on a link to an online article on Facebook about corruption charges of the Zakat (“philanthropy”) Unit in the government of Northern Kordofan.\textsuperscript{61} They were arrested for a day, released after interrogations,\textsuperscript{62} then rearrested again shortly after and charged with defamation.\textsuperscript{63} Details of their conviction are unknown as of mid-2014.

\textsuperscript{58} “Sudan's top court reverses newspaper closure amid continued crackdown on press,” \textit{Sudan Tribune}, March 5, 2014, \url{http://allafrica.com/stories/201403060770.html}.
\textsuperscript{59} Based on author interview. June/July 2013.
\textsuperscript{61} Based on FOTN Sudan analyst's research on the ground.
\textsuperscript{62} “Sudan security questions group of youths over Facebook posts,” \textit{Sudan Tribune}, July 9, 2013, \url{http://www.sudantribune.com/spio.php?article47241}.
\textsuperscript{63} Author's Research.
Sudan

During the September 2013 protests, the pro-democracy group Sudan Change Now (SCN) came under heavy attack by the NISS, with more than ten of its members arrested and kept in detention for weeks, including Dahlia Al-Roubi, a social media activist and SCN member, who was arrested and held for a week; she was released without charges. At least four journalists were detained during the protests, including two women. In another case, Samar Mirghani, a pharmacist and Khartoum University graduate, was arrested while filming the police shoot a young male protester with her phone during the September protests.\(^{64}\) She was later tortured in detention and had her phone confiscated for the alleged possession of “indecent” materials. Her trial received a significant amount of national attention, and on October 28, 2013, she was found innocent of the charges lodged against her under article 153 of the penal code (obtaining and having indecent content on her mobile phone) and article 69 (disturbing the public peace), though she received a fine of SDG 5,000 (US$1,120) for participating in the protests\(^{65}\)

The government actively monitors internet communications, and the NISS regularly intercepts private email messages.\(^{66}\) The Sudan Police Department also monitors internet cafes to make sure users do not access websites deemed immoral by the authorities.\(^{67}\) Government surveillance of online activists and journalists was particularly pronounced during the June and September 2013 protests. Meanwhile, mobile phones have become an especially dangerous tool for activists given the widespread suspicion that the authorities possess phone-tapping and location tracking tools.\(^{68}\)

In November 2013, the Al-Arabiya TV channel hosted a show interviewing Mubarak Mohamed, a former officer who worked for the NISS, during which he stated that 80 percent of NISS’s intelligence gathering is collected through phone tapping, although he was not specific on what the phone surveillance entails.\(^{69}\) In one notable incident during the September 2013 protests, three members of Sudan Change Now were arrested shortly after they turned on their mobile phones while in public, raising concerns that activists were being tracked.\(^{70}\)

Mobile phone tapping and tracking was made more feasible in 2008 when a law was enacted requiring subscribers to register their SIM cards with providers. Nevertheless, it was still relatively easy to purchase a SIM card without providing personal information for activation until the June 2012 protests when the policy became more strictly enforced, particularly by the partially government-owned telecom, Sudani.\(^{71}\) Activists believe the effort to be a strategic move by the authorities to track user phone numbers and personal information.

After the September 2013 protests, the campaign to register SIM cards became more aggressive, involving television, newspaper, and billboard advertisements; public mobile registration services; and lotteries to win prizes such as money, gold, or cars. The provider MTN even advertised that users could register their friends’ SIM cards for them. Registration requires a copy of a national ID

---

\(^{64}\) Author’s Research.


\(^{67}\) OpenNet Initiative, “Internet Filtering in Sudan.”

\(^{68}\) Interview in Khartoum, Sudan, August 1, 2012.

\(^{69}\) Author’s Research

\(^{70}\) Author’s Interview with SCN representative, Khartoum, January 2014

\(^{71}\) Based on author’s research.
and home address details. In April 2013, a representative from the NISS told the press that there were 700 police cases a day against unregistered numbers or numbers registered under false names.72

Government requests for user data on international communications platforms such as Facebook have been on the rise in recent years. Between July 2013 and June 2014, a total of five requests were made by the government for information on five separate user accounts on Facebook, compared to zero requests the previous year; none of these requests were granted.73

According to recent research, Sudan has acquired high-tech surveillance equipment. In June 2013, Citizen Lab traced the U.S.-based Blue Coat Systems—which manufactures devices that can be used to monitor network traffic and filter content—to three networks inside Sudan, including on the networks of the private telecom provider, Canar.74 These revelations made evident that the U.S. sanctions regime against Sudan have not impeded the Sudanese government from gaining access to or purchasing U.S.-made surveillance software, as intended. Rather, the sanctions more often impinge upon regular users’ access to ICTs, albeit unintentionally, as discussed above. Meanwhile, Blue Coat Systems claimed that the devices reached embargoed countries without their knowledge.75

Facebook is widely monitored and used to track and incriminate activists for arrest.76 During recent protests, for example, the social media platform was the first website detainees were asked to open while in detention, and private messages as well as the pages that activists “like” were checked to see if they were affiliated with a certain political party or social movement. Consequently, many young people have stopped posting personal pictures on their profiles and changed their Facebook names to pseudonyms to avoid being identified. Testimonies of detained activists have also revealed that the authorities possess pretty sophisticated technical abilities, with one detained SCN member recounting how his MacBook had been confiscated and broken into, despite his refusal to provide his password details.77

Sudanese dissidents living abroad have also been targeted by the NISS, indicating a level of surveillance that may be able to cross international borders or entail cooperation with other governments. The prominent Sudanese blogger, Amir Ahmed Nasr, was one such expatriate who was confronted by an apparent Sudanese security agent while living in Kuala Lumpur, Malaysia. Also known for his autobiography about his blogging experience on difficult questions about Islam, identity, and Middle Eastern politics—which is banned in Malaysia—Nsar was told by the security agent that he was “being watched back in Khartoum by the NISS, and that [he] should

---

77 Author’s Interview with SCN representative, Khartoum, January 2014.
stop [his] articles and speeches against the NCP, or else there will be consequences."\textsuperscript{78} The blogger subsequently left Malaysia to seek political asylum in Canada.

Extralegal intimidation is also a tactic regularly employed by security agents within Sudan, as visibly demonstrated when the government shut down a popular TEDxKhartoum event in May 2013.\textsuperscript{79} Despite months of preparation that included support from a number of government institutions, security agents obstructed the event minutes after it began, threatening to revoke the organizers’ permit and later cut off the facility’s electricity. Because the event had no political agenda, the main organizer of TEDxSudan, Anwar Dafa-Alla, believed that the government was nervous about the event being live-streamed. Dafa-Alla later participated in the September 2013 protests and subsequently left Sudan to seek political asylum in the United States, after being told by a government insider that his name was on a “shoot-to-kill” list.

Journalists and civil society groups have been subject to an increasing degree of technical violence. Online news outlets such as \textit{Al-Rakoba}, \textit{Sudanese-Online}, and \textit{Hurriyat} frequently experience hacking attacks by what activists believe is the work of the Cyber Jihadist Unit.\textsuperscript{80} The webmaster account of the \textit{Sudan Tribune} website was most recently hacked in April 2014, which resulted in the disabling of all staff passwords and the posting of a fake news article on the site about the assassination of the South Sudanese leader, Riek Machar.\textsuperscript{81} Later in April, the opposition website “3ayin”\textsuperscript{82} was hacked by a group calling itself Haras al Hudoud (or “soldiers of the frontier”), whose name appeared on the screen when users tried to access the hacked site while it was down. 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. In October 2013, GIRIFNA (a non-violent youth-based resistance movement) suffered a hacking attempt on its website. According to the group's IT team, the attempt was a phishing attack that tried to trick users into giving up their passwords by directing them to a fake mirror website.\textsuperscript{83}

Individual Facebook pages are also frequently targeted for attacks. In October 2013, for example, Khalid Ewais, a Sudanese journalist working for the UAE-based \textit{Al-Arabiya} channel, reported on his Facebook page that his account had experienced a failed hacking attempt.\textsuperscript{84} An inside source who formerly worked at the Cyber Jihadist Unit revealed that the Unit's practice of Facebook hacking typically begins with the creation of a fake account using a "girl's name and picture to discredit information on pages or to add activists to gain access to their pages."\textsuperscript{85} Sometimes the fake profile

---

\textsuperscript{78} Author’s interview with Amir A. Nasr. Via email. January 16, 2014.
\textsuperscript{80} Interview with Newspaper Owners/Editors, January 2013 - January 2014.
\textsuperscript{81} “Sudan Tribune website hacked; Machar not target of assassination attempt,” \textit{Sudan Tribune}, April 2, 2014, \url{http://www.sudantribune.com/spip.php?article50505}.
\textsuperscript{82} \url{http://www.3ayin.com/} is the Arabic off-shoot of "Nuba Reports" that specializes in collecting video footage and reports from a team of citizen journalists in the Nuba Mountains to disclose information linked to the civil war there and especially its impact on civilians.
\textsuperscript{83} Reem Abbas, “The Online War in Sudan,” Doha Center for Media Freedom, October 30, 2013.
\textsuperscript{84} Reem Abbas, “The Online War in Sudan,” Doha Center for Media Freedom, October 30, 2013, \url{http://www.dc4mf.org/en/content/online-war-sudan}.
\textsuperscript{85} Anonymous interview.
Sudan

has the same name and picture as one of a user’s friends and usually does not have many of its own friends.86

In response to increasing technical attacks against activists in recent years, a hacktivist group known as AnonSudan emerged in September 2013 when it hacked several government websites, including the government’s main site,87 the presidency’s site, and a number of ministerial sites. The group proudly announced on Twitter that it had taken down 149 websites affiliated with the government.88

87 Government of Sudan website: http://sudan.gov.sd
Syria

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>25</td>
<td>26</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>36</td>
<td>37</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>85</td>
<td>88</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 21.9 million
Internet Penetration 2013: 26 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- With the telecommunications infrastructure in a dire state, government agencies and rebel forces continued to periodically shut down internet service to thwart citizen journalism and communications among fighters (see Obstacles to Access).
- Websites that express criticism of the government or opposition viewpoints are blocked (see Limits on Content).
- Activists, bloggers, and citizen journalists that document human rights violations online faced arrest and kidnapping by both the regime and rebel forces such as the Free Syrian Army, al-Nusra Front, and Islamic State of Iraq and the Levant (ISIL). Syrian journalist Abdulwahab Mulla, known for his satirical show on YouTube, was abducted by masked men in October 2013 while in a rebel-held area of Aleppo (See Violations of User Rights).
- Authorities still supply progovernment hackers with servers and data to target online activists with surveillance malware. The Syrian Electronic Army continued to target foreign media outlets for their coverage of the conflict (see Violations of User Rights).
Introduction

Syria remains one of the most repressive and dangerous environments for internet users in 2014. Authorities employ sophisticated technologies to filter political, social, and religious websites, and to conduct surveillance on citizens. Phishing, spear-phishing, and other cyberattacks have grown dramatically over the past year. Progovernment hackers have infected over 10,000 computers with surveillance malware, which can then be used to gain sensitive information about opposition networks or ordinary citizens. 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 (ISIL), whose power has increased over the past year. 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, with more than one-fifth of the population online by 2010. However, the regime has maintained tight control over information and communication technologies (ICTs) for many years by dominating key networks via government-linked service providers and engaging in extensive blocking of websites. Syrian users had limited access to secure connections; the Secure Sockets Layer (SSL) protocol necessary for browsing “https” sites was blocked until 2004, when foreign email providers were finally allowed into the country.

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.

Obstacles to 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 Homs, Daraa, and Aleppo, as they were subject to severe shelling by the Syrian armed forces. By the end of 2013, the International Telecommunications Union (ITU) estimated that 26.2 percent of the population had access to the internet. The number of fixed broadband subscribers increased to 346,000, a ten-fold increase from 2009 but still representing only 1.58 subscriptions per 100 inhabitants. Mobile phone penetration was at about 56 percent.

In 2009, mobile phone companies began providing 3G services in Syria, though the number of subscribers had reached only 80,000 by late 2010 due to the relatively high prices, almost US$25 for 4 GB and US$200 for unlimited data usage. In addition, the service is primarily available in large cities. Most users connect to the internet through a fixed dial-up connection at speeds of only 56 Kbps, which severely limits their ability to download or view multimedia content. During peak times, the speed is even slower. Broadband ADSL service remains limited due to the inadequate infrastructure in rural areas at prices which remain beyond the reach of most Syrians. For example, according to a price list published by the Syrian Computer Society, the monthly cost for a connection speed of 1 Mbps was SYP 1650 (approximately US$15) as of May 2012, in a country where gross domestic product per capita, when taken on a monthly basis, is only $274. As two-thirds of the country is disconnected from Syrian internet service providers (ISP) networks, access has declined with the average Syrian unable to afford satellite internet, the most popular alternative.

The country’s connection to the international internet remains centralized and tightly controlled by the government. This is done under the purview of the Syrian Information Organization (SIO) and the state-owned Syrian Telecommunications Establishment (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. 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 STE also serves as an ISP. Private ISPs like Aya, as well as mobile

---

8 See the Ministry of Telecommunications and Technology’s website (in Arabic) at: http://www.moct.gov.sy/moct/?q=ar/node/58.
phone internet providers, are required to sign a memorandum of understanding to connect via the gateways controlled by the SIO. 10

At least 11 ISPs have entered the market since the end of 2005, raising the total number of ISPs to 14. 11 Independent satellite connections are prohibited, although in reality, they are heavily employed due to the unreliability of government ICT infrastructure. 12 ISPs and cybercafes must obtain approval from the STE and pass security vetting by the Ministry of Interior and other security services. 13 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.

During late 2013 and early 2014, 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. Syrians faced a 19-hour internet blackout from May 7 to 8, and an 11-hour shutdown on May 15, 2013. 14 State sources blamed the outages on technical failures, although many speculated that the outages were timed to coincide with a specific political or military purpose. 15 Two shutdowns also occurred in November 16 and December 2012. 17 More localized, but longer lasting cut-offs were reported in seven provinces across the country. This includes, for example, a full shutdown in Aleppo on August 11, 2012. 18

As a result of the devastating conflict, most of the northern and eastern parts of the country have experienced heavy damage to telecommunications infrastructure. Exchange centers have been shelled or deliberately sabotaged by both rebel and progovernment fighters, often to disable the telecommunications network of the other party. This occurred in the cities of Der el Zor, al-Hassaka, and Qamishli, where inhabitants have been offline since May 2013. The government has claimed this is due to technical problems, but reporters believe it is for political reasons. 19 According to activists, broadband is often throttled and 3G services shut off as pro-regime forces prepare to besiege a city. 20 From opposition activists to jihadists, rebel fighters to the Syrian army, all players in the conflict rely heavily on the internet, whether for its use as a propaganda tool or for standard

20 Interviews with several activists in Syria wishing to remain anonymous, August 2011 to March 2012.
communication. As such, many have taken to satellite technology to ensure that blackouts, sabotage, and destruction do not impede their ability to connect.  

**Limits on Content**

The Syrian government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs. 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. The Syrian government is suspected of possessing sophisticated technologies for filtering and surveillance, and 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. Many websites have also been blocked more recently, such as the magazine *Syria Oxygen* and the site *SyriaStocks*.  

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 “.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.” 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 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, that was then sent to Area SpA, believing the equipment would be given to the Iraqi government, but logs obtained by the hacktivist group Telecomix in August 2011 revealed evidence of their use in Syria instead. 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. Analysis of the exposed Blue Coat logs revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites. 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.

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.

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. Websites used to mobilize people for protests or resistance against the regime, including pages linked to the network of Local Coordination Committees (LCCs) that have emerged, continue to be blocked. An online initiative to gather information and raise public awareness, the Mondaseh website, also remains blocked. Websites that document human rights violations, such as the Violations Documentation Center, remain blocked. Authorities have repeatedly blocked the website and key search terms of “SouriaLi” an internet radio station started by a group of pluralistic young Syrians.

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 show a TCP error. The video-sharing website YouTube was also unblocked, although it was not usable from mobile phone devices due to limits on data speeds. 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

31 LCCs website: http://www.lccsyria.org/en/
32 The Syrian, the English page is available at: http://english.the-syrian.com/
35 Interview with activist in Syria wishing to remain anonymous, December 2011.
the sites appear in the Top 25, perhaps due to users employing proxies that change their IP address to another country. 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 government 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 “reboot” 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.

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 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 ISIL or other extremist groups have stepped up their self-censorship in order to avoid criticizing the militants or Islam.

---

41 Email communication from a Syrian blogger. Name was hidden.
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 “Violations of User Rights”). 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 U.S. 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.

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 for a democratic transition and the stepping down of President Assad. He was released one month later.

In addition, one observer has called 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. Indeed, as the Syrian government shifted to the use of heavy arms

---

43 Guy Taylor, “After the Damascus Spring: Syrians search for freedom online.”
45 Guy Taylor, “After the Damascus Spring: Syrians search for freedom online.”
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. Since full media coverage throughout the country is very difficult, citizen journalists have designed a technique to ensure full media coverage of the entire country. “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.

Controversially, both Facebook and YouTube have removed content related to the Syrian uprising under the justification that content posted to the 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 Local Coordination Councils, or 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.

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, at times, rebel fighters. 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.

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.” 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. In addition, Syria’s cybercrime law allows prison sentences of up to three years and fines of up to SYP 250,000 (US$ 1,500) for anyone who incites or promotes crime through

---

51 See http://onsyria.org/.
54 Article 378 of the Syrian Penal Code.
computer networks. \(^5\) The judiciary lacks independence and its decisions are often arbitrary. Some civilians have been tried before military courts.

Since antigovernment protests broke out in February 2011, the authorities have detained hundreds of internet users, including several well-known bloggers and citizen journalists. However, 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. \(^5\) 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. \(^5\) 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. \(^5\)

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. \(^5\) Authorities raided the offices of the Syrian Center for Media and Freedom of Expression (SCM) in February 2012, arresting 14 employees. \(^5\) One SCM member and civil rights blogger, Razan Ghazzawi, \(^5\) was detained for 22 days. \(^5\) 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. \(^5\) The organization’s founder and director, Mazen Darwich, has been held incommunicado since his arrest. \(^5\)

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. \(^5\) 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

---

\(^5\) http://www.fosigrid.org/middle-east/syria


\(^5\) Email communication with activist in Syria who wished to remain anonymous, April 2012.


\(^5\) An interview with Syrian blogger via Skype. February 2013, name is hidden.


\(^5\) Skype interview with Syrian activist, March 2013. The name is hidden.

\(^5\) Interview via Skype with A.A, Human Rights Lawyer in Damascus, December 12, 2011. Name is hidden.
Syria

gone into hiding and dozens have fled the country, fearing that arrest may not only mean prison, but also death under torture.66

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, activists and photographers were targeted by FSA fighters more than they were targeted by the Syrian government.67 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 them for filming a protest in Bostan al Qaser in Aleppo.68

According to Reporters Without Border, at least 51 netizens and citizen journalists were killed between May 2013 and May 2014. In one case from December 2013, the “Islamic State of Iraq and the Levant” (ISIL), an armed extremist group, killed 50 prisoners, including many journalists and media activists such as Syrian journalist Sultan al-Shami.69 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 ISIL, are behind the kidnappings.70 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.71

Competition among activists has also led to violations against each other. In one 2013 case, a citizen journalist used armed thugs to kidnap the administrator of a Facebook page for a competing media groups, aiming to shut it down. The victim sought help from another armed group, who, in turn, abducted the first individual. Both of the kidnapped group administrators were beaten to provide passwords of their Facebook accounts. Eventually, both men were released.72

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.73

66 Interviews with two photographers who have taken refuge in Turkey, December 2011.
67 Interview with activist from Aleppo, via Skype, January 2013. Name is hidden.
68 Interview with lawyer from Aleppo. Istanbul, Turkey. January 2013. Name is hidden.
72 The author helped mediate this case, which occurred in the Damascus suburban area in February 2013. Names are hidden.
73 Interviews with released bloggers, names were hidden.
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 between SYP 100,000 and 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.

Surveillance is widespread in Syria, as the government capitalizes on the centralized internet connection to intercept user communications. 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.\textsuperscript{81} 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.\textsuperscript{82}

A report from Kaspersky Labs, published in August 2014, revealed that some 10,000 victims’ computers had been infected with RATs some 10,000 victims in Syria, as well as in other Middle Eastern countries and the United States.\textsuperscript{83} 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.

Cyberattacks have become increasingly common in Syria since February 2011, in response to the growing circulation of anti-Assad videos and other content online. Most notable has been the Syrian Electronic Army (SEA), a hacktivist group that emerged in April 2011. Though the 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;\textsuperscript{84} a June 2011 speech in which the president explicitly praised the SEA and its members;\textsuperscript{85} and positive coverage of the group’s actions in state-run media.\textsuperscript{86} The SEA’s main activities include hacking and defacing Syrian opposition websites and Facebook accounts, as well as targeting Western or other news websites perceived as hostile to the regime. However, some foreign websites from the academic, tourism, or online marketing sectors have also been targeted.\textsuperscript{87}

A huge shift in the level of hacking operations happened at the end of 2013, when the SEA was able to hack the \textit{New York Times} website,\textsuperscript{88} the U.S. Marines website,\textsuperscript{89} Facebook,\textsuperscript{90} 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

\begin{footnotesize}
\begin{tabular}{ll}
\textsuperscript{82} & “Syrian Malware” Up-to-date website collecting the malware \url{http://syrianmalware.com/} \\
\textsuperscript{83} & For the full report, see “Syrian Malware, the evolving threat,” Kaspersky Lab Global Research and Analysis Team, August 2014, \url{https://securelist.com/files/2014/08/KL_report_syrain_malware.pdf}. \\
\textsuperscript{84} & The Syrian Electronic Army, \url{http://syrian-es.com/}.
\end{tabular}
\end{footnotesize}
(OFA), was briefly hacked by the SEA, resulting in the account posting shortened links to SEA sites.\textsuperscript{91} 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.\textsuperscript{92} The Mondaseh website was also hacked by the SEA in early January 2012.\textsuperscript{93} The SEA is known to post private information, such as the phone numbers and addresses of antigovernment activists, on Facebook.\textsuperscript{94} Most of its pages have been closed by Facebook for violating terms of use. However, progovernment media outlets continue to publish hacked emails from opposition figures. These tactics continued in 2014 with the high-profile hacking of \textit{Forbes} in February.\textsuperscript{95}

\begin{itemize}
\item \textsuperscript{91} "The Syrian Electronic Army Hacked Obama's Twitter Links And Campaign Emails," Tech Crunch, October 28, 2013, \url{http://techcrunch.com/2013/10/28/obamas-twitter-links-and-campaign-emails-were-hacked-by-the-syrian-electronic-army/}.
\item \textsuperscript{92} Max Fisher, "Syria's pro-Assad hackers infiltrate Human Rights Watch Web site and Twitter feed," Washington Post, March 17, 2013. \url{http://wapo.st/1eU9nKf}.
\item \textsuperscript{93} See YouTube video by SEA celebrating the hacking: \url{http://www.youtube.com/watch?v=48q34HlIBOk}.
\end{itemize}
Thailand

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>Not Free</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>60</td>
<td>62</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>60</td>
<td>62</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 66.2 million
Internet Penetration 2013: 29 percent
Social Media/ICT Apps Blocked: Yes
Political/Social Content Blocked: Yes
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Days after the May 2014 coup d’état, military authorities canceled the constitution and issued orders to censor online news, arrest critics, and prevent dissenters mobilizing on social media. Crimes related to lèse-majesté, national security and infringing orders issued since May 25 will be tried by a military court (see Editor’s Note).

- Thousands of internet users lost access for an hour in November when protesters vandalized telecommunications infrastructure (see Obstacles to Access).

- In a first for Thailand, a court jailed an internet user for over six years for “attempting to commit lèse-majesté” via computer, a charge without legal basis (see Violations of User Rights).

- Though the number of censored URLs appeared to decline, court orders now authorize ICT officials to block similar content on other websites without seeking fresh permission, bypassing a legal requirement (see Limits on Content).
Editor’s note

Internet freedom, though curtailed in 2014, remained comparable to the previous coverage period until May 20, when 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 weeks following, 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 Those that took effect before May 31, 2014, and immediately after, are outlined in special sections of Limits on Content and Violations of User Rights.

Introduction

In 2013 and 2014, as Thailand’s intensifying political conflict spilled into virtually every aspect of life, internet freedom ebbed and flowed along with overall stability. Since the 2006 military coup, both the supporters of ousted Prime Minister Thaksin Shinawatra and their opponents have used online resources, particularly social media, to mobilize up to and beyond the 2011 election, when Thaksin’s sister Yingluck Shinawatra, became prime minister. In late 2013, however, political dissent took the form of crippling antigovernment protests under a movement known as the People’s Democratic Reform Committee (PDRC). Yingluck Shinawatra dissolved parliament on December 8, 2013, paving the way for new elections. The PDRC, which had called for a people’s council instead, escalated the protests, fearing that the “Thaksin regime” would return to power. Thousands of protesters stormed key state agencies and vandalized telecommunications infrastructure, severing internet access for several hours.

For their part, the besieged authorities view the online space as rife with rumors and other content that threatens national security. The state has ample means to infringe users’ online freedoms in the form of computer-related crimes laws enacted after the 2006 coup, criminal defamation charges, and oppressive lèse-majesté provisions in the penal code which punish criticism of the nation’s revered monarchy. The state has 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.

On the surface, censorship appeared to decline in 2013, when 58 court orders blocked access to 5,369 URLs, down from 20,000 the year before. In practice, the orders offered information officials the power to independently assess other websites for related content violations and implement blocks without going through the courts, though this step is a legal requirement. This development further complicates the task of tracking government censorship, which already lacks transparency. The political upheaval also had an impact on online content, as rival political factions organized their supports to file mass complaints against their opponents’ Facebook pages. As rumors of a possible coup spread online, officials and police reiterated 2011 threats that “liking” or sharing antigovernment content via social media would be punishable by law, sparking civil society criticism.

The risk of prosecution was keenly felt in 2013 and 2014, as Thai journalists, activists, and social media users faced criminal charges for defamation and insulting the monarchy in online communication. One judgment was of particular concern. In December 2013, an internet forum user with the online name Kenji was jailed for 13 years for “attempting” to commit lèse-majesté online—which has no foundation in Thai law—based on anti-royal content that was never distributed, but found on an electronic device in his home. The sentence was reduced after he confessed to the crime.

Obstacles to Access

Internet access in Thailand continues to increase, thanks largely to the prevalence of smartphones. In 2013, a government source reported internet penetration at 37 percent. Mobile penetration topped 120 percent in 2012, indicating some citizens own more than one device. By 2013, the number of smartphone users in Thailand totaled 34 percent of mobile phone subscribers, a significant increase from 19 percent the year before.

Thailand’s international bandwidth usage amounted to 708 Gbps, and domestic bandwidth amounted to 1,492, 53 percent and 48 percent higher than the previous year respectively. Thailand’s transition from internet protocol (IP) version 4 (IPv4) to the updated IPv6 is making steady progress. On June 4, 2013, the Thai cabinet ordered every state agency to accommodate IPv6 by December 2015, and every internet service provider must be IPv6-compliant by December 2014. The Ministry of Information and Communication Technology (MICT) is tasked with administering the IPv4-to-IPv6 transition plan smoothly to minimize impact on existing internet users.

---


Thailand

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.  

The government has tried to improve access to devices and hardware through projects like the MICT program One Tablet per Child, which aims to distribute free tablets loaded with education software to all first-year primary school students. Critics argue the program distracted public attention away from other factors affecting education, such as poor teacher performance. Thailand’s Office of the Auditor General is investigating news reports that up to 30 percent of tablets involved could be broken.

Two MICT programs to address the digital divide continued in 2013. The Smart Network program aims to expand high-speed internet or broadband coverage to 95 percent of the country by 2020. The ICT Free Wifi 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 their national identification numbers for 20 minutes of free access per session, up to two hours per day. To date, this program has installed 120,000 access points countrywide in collaboration with select ISPs, and aims to install 150,000 more before it ends in 2015. Thailand’s media and telecom regulator, the National Broadcasting and Telecommunications Commission (NBTC), has its own Universal Service Obligation program, which aims to install high-speed internet and public telephones nationwide. In 2013, it launched pilot projects in northern Pitsanulok and northeastern Nong Kai provinces.

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 ($6.73) a month. Connections reportedly function at speeds around 12 Mbps, most reliably in the greater Bangkok area. In recent years, the Thai telecommunications market has liberalized and diversified. Out of nine National Internet Exchanges that connect to international networks, the government-run Communication Authority of Thailand (CAT) Telecom operates two, including the country’s largest. As of

---

mid-2014, there were over 100 ISPs with active licenses, though 10 provided most of the connection services for individual consumers and households. Among them, True Internet—a subsidiary of the communications conglomerate True Corporation, which also controls Thailand’s third-largest mobile phone operator True Move—had a 40 percent share of the high-speed internet market by 2013; the state-owned Telephone Organization of Thailand (TOT) controlled 33 percent in 2012, while the private 3BB controlled 28 percent. The three main mobile phone service providers are the Singaporean-owned Advanced Info Service, the Norwegian-controlled DTAC, and True Move. The first two operate under concessions from TOT and CAT, an allocation system that does not entirely enable free-market competition.

The government does not openly block or throttle internet and mobile connections for political or security reasons, though access was temporarily curtailed in 2013 because of political unrest. On November 30, PDRC protesters blocked the entrances of government buildings, broadcasters, and CAT Telecom. A group vandalized circuits and backup generators at CAT’s Internet Data Center subsidiary, which provides servers and internet telephony services and oversees Thailand’s largest international and domestic gateway hubs; the company also hosts the system which connects every Thai telecom company’s fiber-optic networks. The protesters severely disrupted communication channels, including internet connections. Electricity was down for one hour, severing internet access for 750,000 users nationwide.

The NBTC, which regulates the industry, is made up of 11 commissioners appointed by the senate in 2011. Five are from the military, reflecting the army’s deep interests in the communications sector. The remaining members are three former bureaucrats, two civil society representatives, and one police officer.

Some observers have complained that the NBTC lacks commissioners with industry experience, that the regulatory structure is incapable of dealing with converging communications platforms, and that coordination across different parts of the commission is weak. Others complain the body is difficult to monitor and slow to release information. The three largest operating expenses of the NBTC

20 Both CAT Telecom and TOT are supervised by the MICT.  
22 “Suthep announced total takeover of Government Center, CAT Telecom, TOT – 1 December will be "Victory Day"” (in Thai), Prachatai, November 29, 2013.  
23 Icez (pseudonym) “Why internet countrywide was disrupted when electricity was cut at CAT Telecom building in Bangrak district” (in Thai), Blognone, December 2, 2013.  
24 “Update on the impact on Internet access from protestors cutting electricity at CAT building” (in Thai), Prachatai, November 30, 2013.  
25 Lew (pseudonym), “Suthep does not want government to be able to issue orders via Internet network; TOT electricity is now also out”, Blognone, November 30, 2013.  
in 2012 were donations (to various foundations for philanthropic purposes), travel expenses abroad, and public relations; these three items totaled 40 percent of the annual operating budget.\(^{28}\)

Despite these shortcomings, the NBTC’s decisions have been broadly viewed as fair.\(^{29}\) However, political and legal disputes delayed the NBTC’s licensing process for 3G mobile phone service and wireless broadband until 2012.\(^{30}\) Auctions for the faster 4G spectrum met similar hurdles in the past year. Instead of holding them on schedule in September 2013, the NBTC extended existing spectrum concessions in the 1800 MHz band which would be utilized for 4G for one more year. Dr. Duenden Nikomboriraks, researcher at the Thailand Development Research Institute and herself a member of the NBTC’s telecom consumer protection subcommittee, publicly criticized this decision as against the public interest. In response, four commissioners on the National Telecom Commission (NTC), which is the sub-board of the NBTC (all commissioners sit on the NBTC board), sued her for defamation in late 2013. The criminal court accepted the case, and trial began in June,\(^{31}\) but was reconciled and concluded in September.\(^{32}\)

### Limits on Content

#### May 2014

From the eve of the declaration of martial law on May 20, 2014 and onwards, digital content was particularly curtailed.\(^{33}\) On May 21, the Peace and Order Maintaining Command (POMC) chaired by General Prayuth—which later became the NCPO—prohibited any “reporting of news in documents, pictures, publications, [and] broadcastings,” as well as “distorted online news reports” which could cause social division and unrest, or messages causing widespread fear.\(^{34}\) On May 22, 2014, television and radio channels were ordered to cease all regular programming, including international satellite news. Television screens showed the logo of five army and police units against a blue background. Many news media ceased television and radio broadcasts, but continued to distribute news online. Thailand’s sole public television operator ThaiPBS, which broadcasts mainly through terrestrial television, carried on live news reporting though its YouTube channel.

---


\(^{31}\) “Court accepts libel case: NBTC sues Dr. Duenden, Nattha” (in Thai) Thairath Online, 18 March 2014, [http://www.thairath.co.th/content/410629](http://www.thairath.co.th/content/410629).


\(^{33}\) Order of the Peace and Order Maintaining Command (POMC), Thairath, May 21, 2014, [http://www.thairath.co.th/content/424255](http://www.thairath.co.th/content/424255).

Such efforts were short lived. On the night of the coup, soldiers marched to ThaiPBS station and ordered broadcasting to cease, then escorted Vanchai Tantivitayapitak, the station's deputy managing director, to an army camp. He was released several hours later.35

On June 2, new orders instructed online media to stop propagating content that could cause social division or face immediate suspension.36 The NCPO ordered ISPs to report to the NBTC.37 Other orders cemented media control, barring journalists from inviting anyone other than tenured public officials to “express opinions that will cause social division” in interviews38 and prohibiting all media from disseminating false news, slander, instigating antiroyal sentiment, or criticizing the NCPO.39

A number of free terrestrial televisions networks returned to broadcasting on May 23.40 Digital television networks were allowed back on air the following day, but prohibited from screening call-in shows or viewer comments submitted via SMS.41 Some subscription-only cable networks had to suspend foreign news channels because they could not control their content to comply with NCPO orders.42 A handful of satellite television networks were allowed back on June 4,43 while several channels that focus on political news and commentary, such as Voice TV and T-News, returned on June 14 on condition that they observe NCPO orders.44

At the same time, the junta censored websites reporting criticism of the new regime or documenting alleged human rights violations. The MICT’s permanent secretary told journalists the ministry had blocked access to 219 websites in the week after the coup.45 Some of these targeted specific web pages, like the Thailand page of Human Rights Watch, or a Reuters’ article on Thai censorship. Entire domain names were also blocked, including the news site Prachatai, UK newspaper the Daily Mail, a collection of academic articles called Midnight University, and Enlightened Jurists, homepage

of “Nitirat,” a group of legal experts who proposed amending Thailand’s lèse-majesté law. In some cases, the MICT did not block access but ordered ISPs to suspend a website’s service. This is what happened to political and social news website Prachatham, based in northern Chiang Mai. The censorship of political news was accompanied by a crackdown on illegal gambling, which resulted in the blocking of several sports websites, including at least one that was blocked by mistake.

Any political gathering of more than five people is illegal under martial law. In place of open demonstrations, activists embraced creative expressions of dissent. Some held up three middle fingers to evoke the anti-authoritarian protests depicted in the Hunger Games movie franchise. Others met publicly to eat sandwiches or read. Organizers of these symbolic activities relied on online channels like Facebook and the Japanese chat application Line.

On May 28, 2014, Facebook became inaccessible for approximately 40 minutes across Thailand, except for those using circumvention tools. In a media interview, the MICT permanent secretary said the NCPO temporarily suspended Facebook access to curb violence. That secretary later retracted his account, saying a journalist misunderstood, and that the outage was the result of a technical error. An NCPO order ousted the secretary two weeks later. Separately, however, a spokesman for the Telenor Group, owner of the DTAC mobile network operator, told the Norwegian Aftenposten newspaper that the telecommunications regulator NBTC had ordered mobile networks to block Facebook on May 28. An NBTC official called the comment inappropriate, said foreign shareholder percentages in DTAC would be subject to scrutiny, and threatened to ban DTAC from the upcoming 4G spectrum auction. Telenor issued a public apology for actions which “damaged the public image of the NBTC and the NCPO.”


770 www.freedomhouse.org
May 2013—April 2014

In 2013, Thai Criminal Courts issued 58 court orders to block access to 5,369 URLs. This marks a significant decline from 2012, which saw over 20,000 URLs blocked by court order. However, orders gave ICT officials authority to censor similar content on their own without seeking separate permission. Political groups rallied on Facebook to report their opponents for offensive conduct, effectively disabling rival pages.

The Thai government has been blocking some internet content since 2007, though some controls on pornography, gaming, and other topics were announced even earlier. Article 20 of the 2007 Computer-related Crimes Act (CCA) authorizes MICT officials to request court orders to block content that is deemed a threat to natural security, or contravenes public morals or public order. The Thai government can also censor by means of special laws, such as the State of Emergency Act and Internal Security Act, as they did in 2010.

Since the passage of the 2007 CCA, Thai courts are more likely to censor political opinion than other illegal content. Lèse-majesté or antiroyal content has accounted for 90 percent of censored URLs. Pornography, the next biggest category, accounted for less than 10 percent, while a remaining 0.5 percent of content included religion, violence in southern Thailand, and defamation of public figures [See category “other” in Figure A]. This remained consistent during the 2011 leadership change, even though the number of sites affected appeared to decline. After former Prime Minister Abhisit Vejjajiva came to power, a total of 78,072 URLs were blocked by 129 court orders. From 2011 to 2013 when Yingluck took over, the number of webpages blocked declined to 27,685 URLs based on 237 court orders.

Figure A. Statistics of Website Censorship in Thailand, from 2007-2013

<table>
<thead>
<tr>
<th>Content</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insulting the king, queen, or heir</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obscene or pornographic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abortion pills</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encourage gambling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Depreciate the religion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>1</td>
<td>2</td>
<td>13</td>
<td>64</td>
<td>45</td>
<td>45</td>
<td>58</td>
<td>107,830</td>
</tr>
</tbody>
</table>

58 Journalists sometimes refer to it as the “Computer Crime Act.”
The Technology Crime Suppression Division under the Royal Thai Police, and the MICT's Cyber-Security Operation Center (CSOC) established under Shinawatra in December 2011, are tasked with monitoring and curbing the circulation of lèse-majesté content. Media reports describe the police body as several dozen computer technicians scouring thousands of websites, manually and with automated crawlers, for insults to the royal family. The CSOC is an upgrade of a 2010 entity called the Internet Security Operation Center, but its precise mandate and activities remain unclear. The ministry has also set up a hotline to receive citizen complaints about possible content violations, and operates a “Cyber Boyscout” program, which trains school children to patrol the web for “inappropriate online content,” particularly lèse-majesté.

In addition to blocking websites, ICT officials must prosecute the party responsible for content violations under the CCA. ISPs and content hosts cooperate with court orders, and sometimes implement pre-emptive censorship, to avoid the legal liability more fully detailed in Violations of User Rights. Bigger providers set up teams to monitor and screen users’ posts, and many have removed forums or comment sections altogether, viewing the legal risk as too high.

International providers can be less compliant. Google complied with two requests to delete 14 items on YouTube for criticizing the government in 2012. It received only one such request from the Thai government, pursuant to a court order, in the first half of 2013, but did not fulfil it.

Since February 2012, a troubling proviso has appeared in court orders allowing ICT officials to block access to online content directly if it resembles content already covered in an existing court order, whether the same URL or not. In addition to contravening the CCA, which requires a court to sanction every order, this will make it even harder to track the number and nature of URLs blocked in near future.

The process already lacked transparency. The precise list of inaccessible sites has never been available to the public, and officials may inflate the figures for political purposes. Court orders are

---

64 MICT’s 24/7 hotline “1212” for complaints regarding websites that infringes national security, good morals and Thai culture, or via email: 1212@mict.mail.go.th.  
66 ISPs do not publicly acknowledge such cooperation, but it is widely accepted by freedom of expression advocates.  
69 Case database, Criminal Court (in Thai), http://aryasearch.coj.go.th/aryaweb/.  
70 Some counted duplications, so that a single article shared by ten internet users would be counted eleven times. Interview with mid-ranking ICT ministry employee who requested anonymity, December 2011. In addition, iLaw researchers collecting details of blocked websites in 2012 found many government agencies unable or unwilling to provide data.
granted with minimal deliberation and do not serve as a check on the MICT’s power to ban content. Nonetheless, their existence makes it harder in practical terms for content providers to appeal. The process for officials to petition courts for censorship orders is similar to that for arrest warrants, where the authority rests with a single lower court judge. Two defendants have asked courts to rescind arrest warrants in the past, but the Supreme Court refused, saying the law was not intended to allow pleas which would delay the judicial process, an argument experts believe would apply to censorship orders too.\(^{71}\)

Other legal challenges have yet to yield results. In 2013, a group of law professors from Thammasat University asked the MICT for a copy of the court order that blocked their legal website \textit{Nitirat} for publishing a historical treatise advocating a constitutional monarchy in Thailand.\(^{72}\) The MICT complied, but the URL remained blocked in 2014, though the uncensored treatise is available on other websites. In an unrelated case, the political news platform \textit{Prachatai} sued several government ministers and sought a court order to reverse a 2010 block on its website.\(^{73}\) It was among thousands blacklisted under the emergency declaration in effect from April to December 2010.\(^{74}\) Although some of those sites are now accessible again, others—including \textit{Prachatai} and \textit{Asia Sentinel}—remain at least partially blocked.\(^{75}\) A civil court ruled that the censorship was a proper enforcement of law, and in March 2013 an appeals court declined to reconsider the decision on grounds that the state of emergency had long since been lifted.\(^{76}\) However, the same court ruled that while a suit against individual ministers in the original complaint had no grounds, \textit{Prachatai} was entitled to sue the MICT and the Ministry of Finance. As a result, this case bounced back to the lower courts during the coverage period of this report.

Social networks such as YouTube, Facebook, Twitter, and international blog-hosting services like Blogger are popular and freely available—though individual pages or videos may be blocked—and many political, social, and human rights issues are freely and passionately debated online in Thailand. Such sites have become important spaces for political expression and key channels for disseminating news, information, and demands for accountability. Social media has even facilitated some public discussion of lèse-majesté provisions. The government is also embracing social networks to promote policy. Top leaders update the public frequently on Facebook, especially during election campaigns, though digital tools do not yet have the reach of traditional media, particularly in rural areas.\(^{77}\)

Political groups active on social networks have become adept at using companies’ own terms and standards to censor their opponents, posting URLs containing content deemed to be lèse-majesté


\(^{75}\) Freedom House tests on \textit{Prachatai} and \textit{Asia Sentinel} indicated that the sites loaded more slowly than others and that some pages were inaccessible, with the user redirected to a message stating that it had been blocked by the MICT, though other pages were available.


for members to report to Facebook as hate speech. One group, “Report Society,” was founded with a sole purpose of opposing other pages whose members have tried to adopt the tactic against them by reporting them to Facebook, like the “Coalition for Freedom Protection in Cyber World” page.

Others used social media to broadcast hate speech and disclose others’ personal information to encourage real-world harassment. In mid-February 2014, Thailand’s Civil Court ruled on a lawsuit brought by the antigovernment PDRC against the prime minister and directors of the government’s Center for Maintaining Peace and Order (CMPO, high command set up under the emergency decree). The court ruled that the government has the authority to announce an emergency decree (which took effect between 22 January and 22 March 2014), but no authority to disperse peaceful protesters. After the decision, the judges’ names, home addresses, phone numbers, and car license plate numbers were posted on Facebook. In March, the court’s secretariat office asked police to get the information removed to prevent violence against the judges. The page in question posted the court’s request letter addressed to the police, closed down, and opened another page displaying the same information.

Online activists have proved resilient and creative in countering limits on content. Circumvention software to access blocked sites is readily available online, and content producers often republish information on alternate sites. In 2011, the former ICT minister warned users that “liking” lèse-majesté content on Facebook could result in prosecution for “indirectly distributing inappropriate content” under the CCA, prompting civil society protests. In 2013, police and government officials repeated the warning in relation to rumors of an upcoming coup that circulated on social media in summer 2013 (see Violations of User Rights), and the phrase “liking is not a crime” resurged in popularity online.

On December 9, 2013, Thailand witnessed the largest turnout of anticorruption, antigovernment protesters in its history, a level of mobilization difficult to imagine without social media. Although the protests escalated and were marred by violent incidents, the turnout played a major role in Prime Minister Yingluck’s decision to dissolve parliament and call a snap election.

83 “Clicking ‘Like’ is not a crime; MICT must reexamine how to deal with ‘lèse majeste websites’ and recommendations for netizens who come across websites they don’t like” (in Thai), Thai Netizen Network, November 30, 2011 https://thainetizen.org/2011/11/click-like-is-not-a-crime/.
84 “Clicking ‘Like’ is not a crime” (in Thai), Kom Chad Leuk TV program, August 7, 2013, http://bit.ly/MJM1MK.
Violations of User Rights

May 2014

After the coup, the NCPO made dozens of arrests, stepped up digital surveillance, infringed on online privacy, and created a climate of fear where internet users conducted on- and offline “witch hunts” against fellow citizens.

Within a month after seizing control, the NCPO had detained over 500 individuals, including politicians, activists, academics, and journalists. Over 150 of these had exercised freedom of speech in ways that displeased the junta. Some were summoned via public announcements broadcast on every television channel, while others were subject to unofficial arrests made at homes or workplaces. Detainees were brought to designated military camps around Thailand, where personal communications devices were confiscated. Some were blindfolded to conceal the camp's location. While in custody, individuals were interrogated on their political views. The NCPO said the detentions were carried out under martial law, which authorizes military detentions without legal counsel for up to seven days. Prior to release, the individual in custody would be forced to sign “conditions of release” papers, agreeing not to express political opinion in public, participate in political movements, or travel overseas without NCPO consent, and agreeing they had not been tortured during custody. Many were also ordered to surrender their Facebook account password to the army.

A number of detainees faced criminal charges as soon as the seven day limit was reached. On June 2, NCPO orders stipulated that crimes related to lèse-majesté, national security, or infringing NCPO orders issued after May 25 would be tried by a military court, which lack appellate and higher courts. Three judges conduct military trials, but two are not required to have a law degree if their military ranking is higher than the defendants'.

In this environment, charges of lèse-majesté and computer-related crimes brought by internet users against fellow citizens increased along with political detentions. By June, a civil society group led by a military officer, styling itself the “Rubbish Collection Organization,” had filed charges of lèse-majesté against five internet users with the Technology Crime Suppression Division (TCSD).

In the month after the coup, there were at least five cases of a lèse-majesté charge added when an individual was already in detention. Three notable ones involved digital content:

In May, police arrested a protester identified by the single name Apichat in Bangkok. After seven days in detention, he was charged with violating an NCPO order prohibiting protests. Citing content posted on his Facebook page, a witness separately accused him of lèse-majesté, substantially increasing the possible penalties he faces if convicted.

87 Direct interviews with some individuals who were summoned.
Another telling case involved Sombat Boonngamanong, a prominent activist who has leveraged new media to address issues of missing persons, post-Tsunami recovery, and the 2011 floods. He also founded the “Red Sunday” meetings after the 2006 coup, which encouraged people to independently associate and mobilize without relying on a political party and initiated the pro-democracy red-shirt movement. Sombat refused to cooperate with an NCPO summons issued after the coup, but set up a “Catch me if you can” campaign on his Facebook page. A joint army and police operation arrested him on June 6, apparently having traced him via his IP address. Although he was initially charged with violating an NCPO order by not responding to the summons, police added the charge of lèse-majesté while he was in custody, based on an earlier complaint against him. This prolonged his detention for three weeks before he was released on bail in July.

Chaturon Chaisang, former minister of education, also refused to answer an NCPO summons. Police arrested Chaturon in the middle of a press conference held at the Foreign Correspondents’ Club of Thailand. Shortly thereafter, he was charged with violating Thailand’s Computer Crimes Act for posting anti-coup statements on Facebook.

Online anonymity is under threat since the coup. In late May, the MICT reportedly proposed to establish a single national gateway to the international internet to expedite monitoring and censorship of online content that is deemed illegal. Reports in June 2014 said MICT officials were consulting with vendors to implement the plan, which would require every Thai citizen to authenticate their identity using a smart ID card before logging onto the internet. At the end of June, there were no confirmed developments.

Officials from the Department of Special Investigation announced in May that they were requesting to join private chat groups on the messaging app Line in order to monitor group conversations for inappropriate content. In early June, a senior police official said police have a duty to check Facebook accounts which share anti-coup messages or invitations to congregate. “Liking” illegal content is also considered a criminal offence, as an act of sharing.

Police also used surveillance methods to capture personal data. In early July 2014, many Thai internet users found that visiting blocked websites prompted a screen with a TCSD logo and a message explaining it had been censored. Attempting to close the message triggered a request for consent to share the user’s personal data, apparently through a Facebook app titled Login. Clicking “Agree” automatically compromised users’ Facebook account details. After the Thai Netizen Network publicized this exposure, the “Close” button which launched the fake app disappeared from TCSD messages.

---

and the TCSD website posted an invitation to “Friend” the division on Facebook in order to help them uncover suspicious activity online.96

May 2013—April 2014

As in past years, many Thai journalists, activists, and citizens were sued for defamation and insulting the monarchy in online communication during the coverage period of this report. In an unprecedented case, an internet user known as Kenji was jailed for 13 years for “attempting” to commit lèse-majesté online after police uncovered unpublished anti-royal comments on a device connected to the internet in his home. The sentence was reduced after he confessed to the crime, which has no legal basis. Inadequate technical evidence continues to mar proceedings, and one Prachatai commenter was sentenced to five years in prison for committing lèse-majesté based on misinformation about the computer where the post originated. As rumors of a coup spread online, police tried to persuade international social networks to supply them with user data to assist national security inquiries.

Article 45 of the Constitution of the Kingdom of Thailand 2007 guarantees broad freedom of speech. However, other laws have been used to curtail free expression, including the Internal Security Act of 2007 and the Emergency Decree on Public Administration in Emergency Situations 2005. The 2007 Computer related Crime Act (CCA) groups online speech offenses—such as posting or allowing the dissemination of content considered harmful to national security or public order—with criminal activities like hacking or posting obscene material. Civil society groups and scholars say the CCA can be abused to launch personal or politicized attacks against content providers, webmasters, and other intermediaries.97

Many offences in this law already exist in the penal code, but the CCA carries harsher penalties. Article 14(1) provides for prison sentences up to five years, fines up to THB 100,000 (US$ 3,330), or both for anyone who transfers damaging “forged” or “false” computer data,98 and is often used simultaneously with Articles 326 and 328 of the penal code pertaining to defamation, which carries a maximum sentence of two years in prison or fines up to THB 200,000 ($6,660).99 Under the penal code, only the victim has the right to sue for defamation, which is considered a personal offence. In contrast, anyone can file criminal charges under the CCA, whether or not they are implicated in the disputed content. Moreover, Article 14(1) refers to the illegal tampering with electronic data, so its application to speech is a misinterpretation, according to Surangkana Wayupab, director of the MICT’s Electronic Transactions Development Agency, who is pushing to amend the CCA.100

Police, the attorney general, and the courts continued to pursue such cases during the coverage period of this report. One ongoing investigation dates from February 2013, when the owner of a

98 Research has shown that Article 14(1) is the most-often used Article in this law. Between 2007 and 2011, there were 100 cases brought under Article 14(1), from the total of 325 cases. See, http://ilaw.or.th/node/1798.
99 In Thailand’s judicial system, when someone is charged for offences in more than one law, the court will mandate penalty according to the law in which the penalty is highest, not adding penalties together.
canned pineapple factory sued researcher Andy Hall for defamation and CCA violations in a report alleging the company had violated labor rights. Hall’s findings, sponsored by the Finnish non-profit organization Finnwatch, were publicized on many websites. A few months later, in an April 2013 speech in Mongolia, Prime Minister Yingluck Shinawatra courted controversy at home when she characterized the 2006 coup d’état, when the military displaced the elected caretaker government headed by her brother Thaksin, as a backward step for the country. In May 2013, she sued a prominent political cartoonist who uses the pseudonym Chai Ratchawatra for defamation and CCA violations, after he posted the response, “a whore sells her body, an evil woman sells her country,” on his personal Facebook page. That investigation is also ongoing. Finally, in December 2013 the Thai Navy sued Alan Morison and Chutima Sidasathian, journalists at the Phuket Wan news website in Phuket province, for defamation and violation of CCA Article 14 (1). The previous July, they had cited a Reuters news agency investigation that accused the Thai military of profiting from the illegal smuggling of Rohingya refugees, a persecuted minority in neighboring Myanmar, into Thailand.

Police continue to investigate, though the original article can still be accessed. As of mid-2014, no lawsuit had been brought against Reuters.

Article 14(3) of the CCA prohibits the “import to a computer system of any computer data related with an offence against the Kingdom’s security under the Criminal Code,” and carries a penalty of five years’ imprisonment, a fine of up to THB 100,000 ($3,330), or both. It is often used in conjunction with Article 112 of the penal code, which pertains to lèse-majesté. The first case ever tried under the CCA in 2009 followed this pattern, which persists to this day. Since Article 112 carries jail terms from 3 to 15 years, those charged under both laws face a 15-year maximum.

In September 2013, Porntipa Supatanakul, owner of a cable TV program, sued Saran C., a Thammasat University student pseudonymously known as Aum Neko, for committing lèse-majesté and violating the CCA in an interview that was never broadcast, as well as in personal Facebook posts. On March 24, 2014, police summoned the defendant to hear charges, and the investigation is ongoing. In an unrelated case from September, dozens of police in Samut Prakan province raided the residence of a man using the online username Kenji in the online discussion forum “Internet to Freedom” for allegedly posting two lèse-majesté statements online. After his arrest, police found photos with lèse-majesté remarks on a personal device that can connect to the internet and accused him of “attempting” to commit lèse-majesté—a charge with no legal basis. Nevertheless, in December 2013, a criminal court found him guilty of violating both Article 112 of the penal code and CCA Articles 14(2) and 14(3), sentencing him to a total of 13 years and 4 months in prison. The same court reduced

the sentence to just under seven years because he confessed.\textsuperscript{110} The verdict marked the first time in Thailand that a defendant has been found guilty for attempting to commit lèse-majesté.

Internet users who post controversial content can face harassment outside the legal system, including physical violence. Somsak Jiemteerasakul, an outspoken Thammasat University historian, shares opinions on the monarchy and Thai politics with 80,000 Facebook followers, despite an ongoing lèse-majesté lawsuit the Thai army filed against him in 2011.\textsuperscript{111} On February 6, 2014, the army announced that some of his Facebook posts may also violate lèse-majesté laws.\textsuperscript{112} On February 12, unknown assailants fired multiple shots and hurled bricks at Somsak's car and house while he was inside. No one was injured, but the police investigation into the attack appears to have stalled.\textsuperscript{113}

CCA Article 15 states that administrators who fail to stop internet users from posting banned content are “supporting or consenting to” the post and face the same penalties as if they had created it themselves.\textsuperscript{114} This serves as a discouragement to service providers, since the constant monitoring it demands from website owners is time consuming and inefficient. Moreover, the law fails to establish a time frame for service providers to delete offending content. In 2012, a court sentenced Prachatai’s Chiranuch Premchaiporn to a suspended eight months in jail and a THB 20,000 ($673) fine for failing to delete 10 anti-royal comments,\textsuperscript{115} though the site’s administrator had removed them all within 20 days.\textsuperscript{116} In April 2013, the ICT Ministry published the draft of an amendment to the CCA, including Article 15.\textsuperscript{118} It stipulates that service providers who “know or should know” of computer data on their platforms that violates the law must “remedy the situation,” whether by deleting it or informing the original poster to do so, in order to avoid liability. Like the current law, this puts blame on intermediaries rather than protecting them, and may even lead to more responsibility on grounds that they “should know” of infractions. While the ministry is soliciting public opinions on the draft via an official website, it is not clear if they will be incorporated into the final amendment.

CCA enforcement is inconsistent and lacking in due process. The executive authorities are left to decide what amounts to a violation under its vaguely defined terms, and criminal courts make the final judgments.\textsuperscript{119} Many cases are tried without adequate evidence, and defendants who face attorney generals as plaintiffs often decide not to fight their case, because admitting guilt typically leads to reduced penalties and is the fastest way to end the often convoluted proceedings.

\textsuperscript{110} The actual sentence was 5 years and 20 months.
\textsuperscript{112} “Army displeased; Somsak Jiemteerasakul’ criticisms of the monarchy on Facebook, may be liable under lese majeste” (in Thai), Prachatai, February 6, 2014, http://prachatai.com/journal/2014/02/51646.
\textsuperscript{114} Section 15: “Any service provider intentionally supporting or consenting to an offence under Section 14 within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offence under Section 14.”
\textsuperscript{119} Suksri et al, Impact of the Computer-related Crime Act, 520.
On October 2, 2013, an appeals court sentenced a lèse-majesté defendant to five years in prison. In 2011, a court had dismissed the charge against Nopawan T., the 31-year-old manager of a vehicle parts company, based on statements posted to a Prachatai web forum. Police had traced the IP address behind the statements to a factory where many computers connect to the internet, which the court said was insufficient proof of guilt. The appeals court disagreed and reversed the earlier acquittal.

In a separate case in March 2014, an appeals court upheld a ruling that two messages allegedly posted by former stockbroker Kata P. on the Fah Diew Kan (“Same Sky”) bulletin board violated Article 14(2) of the CCA by connecting a crisis of confidence among investors to rumors about the king’s health. The decision was based on testimony from an MICT official citing information received from Microsoft Thailand that supposedly connected the defendant’s email address to the posts. When first presented to the criminal court in June 2013, the Microsoft Thailand information failed to demonstrate that link, but the MICT official presented it again, and said it was supported by unspecified classified information obtained from security and intelligence agencies. Kata P. is now serving a jail term of two years and eight months.

The CCA was passed after the 2006 coup d’état and has been actively used in subsequent national security investigations, when police are known to implement surveillance. The scale and technical capabilities of their activities are unclear, though the CCA requires ISPs and webmasters to retain data logs for up to 90 days and turn data over to investigators upon request. A cabinet directive effective since its publication in the Royal Gazette in May 2012 placed several types of cases, including CCA violations, under the jurisdiction of the Department of Special Investigation (DSI). Under rules regulating DSI operations, intercepting internet communications and collecting personal data in CCA cases no longer needs a court order. Even where court orders are required, Thai judges typically approve requests without serious deliberation—as is the case with censorship decisions. Some internet users and political activists exercise caution when communicating online, and employ additional security and privacy tools to evade surveillance.

In July and August 2013, rumors of a pending government takeover circulated online. The police’s Technology Crime Suppression Division (TCSD) searched social media posts for the word ‘coup,’ and summoned four people suspected of initiating the report, including Sermsuk Kasitipradit, editor of politics and national security at the public television station ThaiPBS, who had analyzed the rumors on his personal Facebook page. After the summons made headlines and was widely criticized, the division said the individuals were being sought merely as witnesses. In the wake of the rumors, however, both the government Center for Maintaining Peace and Order and the TCSD independently

---

126 Pakorn Peungnet, “Clicking “like” may be a crime!” (in Thai), [Bangkokbiznew](http://www.oknation.net/blog/kobkab/2013/08/13/entry-1)
announced that referring to such rumors or “liking” them on Facebook was tantamount to supporting them, and could be punishable under CCA Section 14(1).\textsuperscript{128} Separately, Facebook disclosed that it had received two requests from the Thai government in the first half of 2013, seeking information on five Facebook users, but did not provide more details.\textsuperscript{129} TCSD Director Pisit Pao-in also said that his team had requested Japan-based Naver Ltd., the owner and operator of the popular Line chat application, release chat logs and information on users for communication that affect national security.\textsuperscript{130} Naver responded that it would only cooperate under a Japanese court order.\textsuperscript{131}

Customers at cybercafes must present identification cards, though smaller businesses do not always comply with this rule. Mobile phone users are required to register their real names and national ID with their carrier upon purchasing a SIM card, whether prepaid or subscription. Although the rule is less strictly enforced for prepaid SIM cards, those who do not register are unable to receive certain services.\textsuperscript{132}

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. In May 2013, a group calling themselves “Unlimited Hack Team!!!” left pejoratives about Yingluck Shinawatra on the Prime Minister’s office website.\textsuperscript{133} In February 2014, anonymous hackers disabled the Office of National Economic and Social Development Board website to prevent them from disclosing economic data, forcing them to release the information to the press via email.\textsuperscript{134}

\begin{itemize}
\item \textsuperscript{128} “Netizens heap blame on MICT – clicking like is not a crime” (in Thai), Mthai, August 6, 2013, http://news.mthai.com/hot-news/260376.html; Pakorn Peungnet, “TCSD to get ‘Line’ data, after saying “Like” clickers may be considered criminals!” (in Thai), August 13, 2013, http://www.eknation.net/blog/kobkab/2013/08/13/entry-1,
\item \textsuperscript{129} Facebook, Global Government Requests Report, https://www.facebook.com/about/government_requests.
\item \textsuperscript{130} “TCSD prepares to control Line, claims affect national security” (in Thai), Voice TV, August 13, 2013, http://news.voicetv.co.th/technology/78551.html.
\item \textsuperscript{131} “Don Sambandaraksa, Naver denies collaborating with Thai govt,” Telecosmasia, August 23, 2013, http://www.telecosmasia.net/content/naver-denies-collaborating-thai-govt.
\item \textsuperscript{134} “NESDB website hacked” (in Thai), Post Today, February 17, 2014, http://bit.ly/1juh21A.
\end{itemize}
Tunisia

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>12</td>
<td>11</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>21</td>
<td>20</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>41</td>
<td>39</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 10.9 million

| Internet Penetration 2013:              | 44 percent |
| Social Media/ICT Apps Blocked:         | No         |
| Political/Social Content Blocked:      | No         |
| Bloggers/ICT Users Arrested:           | Yes        |
| Press Freedom 2014 Status:             | Partly Free |

Key Developments: May 2013 – May 2014

- A new constitution was passed in January 2014 that enshrines the right to free speech, protects the privacy of communications data, and bans “prior censorship” of the media. However, laws on criminal defamation, insulting state bodies, or offending religion remain a threat to free speech and independent reporting (see Violations of User Rights).

- A handful of Tunisians were detained, fined, or sentenced to prison time for their online activities. Journalists faced criminal defamation charges for criticizing public officials, while others, such as rapper Ala Yacoubi and social media user Jabeur Mejri, continue to face legal harassment despite being released from prison on earlier charges related to online expression (see Violations of User Rights).

- The Technical Telecommunications Agency (ATT) was established with a mandate to monitor cyberspace and pursue cybercrimes, sparking fears that censorship and surveillance may return to pre-Ben Ali levels (see Violations of User Rights).
Introduction

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. Despite a relatively advanced internet infrastructure and a developed telecommunications market, extensive internet filtering hindered free web access. Numerous websites and online platforms such as the photo-sharing site Flickr and video-sharing site YouTube were blocked in order to deny citizens access to content critical of the ruling regime. Nonetheless, internet usage continued to grow and an increasing number of netizens started employing encryption techniques and proxy servers to circumvent government censorship and surveillance.

The Tunisian internet 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 web access. In the past three years, authorities have taken significant steps to open up the country's control over information and communication technologies (ICTs), despite attempts to filter pornography in 2012.1 and five Facebook pages critical of the military institution in 2011.2 Over the past year, no internet filtering practices were recorded. To further cut ties with its previous reputation as an “internet enemy,” Tunisia hosted the third edition of the Freedom Online Conference in June 2013,4 after joining the coalition of governments “committed to collaborating to advance internet freedom” in September 2012. A new constitution that protects free speech, bans “prior censorship,” and protects data privacy was passed in January 2014.

Despite these commendable steps, 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, or insults to state bodies. Hakim Ghanmi was fined for defamation over an article he posted regarding a state hospital, while Mourad Meherzi, a cameraman for an online television station, was detained for three weeks after capturing a scene in which a famous actor pelted the culture minister with an egg. Ala Yacoubi and Jabeur Mejri, previously charged over online speech, continue to face legal harassment on new charges that appear trumped up. Meanwhile, fears over unchecked government surveillance were renewed following the creation of a new telecommunication investigative body in November 2013, the Technical Telecommunications Agency (ATT). These developments continue to the country back from achieving further progress in internet freedom and digital rights.

---

Obstacles to Access

Internet usage in Tunisia has grown rapidly in recent years. According to the International Telecommunication Union (ITU), internet penetration stood at 43.8 percent in 2013, up from 27.5 percent in 2008. The number of fixed broadband subscriptions per 100 inhabitants rose to 4.77 by the end of 2013, up from 2.19 subscriptions five years ago. Although the government has actively sought to improve the country’s ICT sector, access is still hindered by high prices and underdeveloped infrastructure.

In 2004, the government set up a “Family PC” initiative to encourage widespread computer use by removing customs fees, setting a price ceiling for computer hardware, arranging low interest rate loans for families to purchase ICT tools, and including an internet subscription with every computer sold. The number of computers per 100 inhabitants rose from approximately 12 in 2009 to 18 as of January 2014, while the number of total internet subscriptions is estimated to have exceeded 1.4 million as of January 2014.

The popularity of mobile phones is also on the rise, with over 12.7 million mobile phone subscriptions and a penetration rate of 115.2 percent as of January 2014. Less common, however, is the use of mobile internet connections due to costs which remain beyond the reach of many Tunisians.

Access to the internet through plug-in USB keys that connect laptops and other devices to 3G networks is on the rise, and at the expense of DSL subscriptions. The number of 3G internet subscriptions reached more than 846,372 in December 2013, compared to 566,337 subscriptions one year ago. Meanwhile, DSL subscriptions decreased from 512,390 to 507,379 over the same period.

---

The three major telecom operators, Ooredoo Tunisia (formerly Tunisiana), Orange Tunisie, and state-controlled Tunisie Télécom provide 3G internet access via USB keys. The device usually costs at least TND 40 (approximately US$ 22), while the service costs TND 30 (US$ 16) per month. Prices differ depending on the operator and the subscription offers clients choose. For instance, Tunisie Télécom has a special offer for students, who can buy a 21 Mbps USB key at 14 TND and pay TND 15 (US$ 8) for 3 GB of prepaid internet access per month. Nonetheless, internet access remains beyond the reach of a large segment of the population. According to a World Bank report released in January, “the poorest 40 percent of the population would need to spend over 40 percent of their income to afford high speed internet.”

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$ 0.55). 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. At the same time, the law restricting the provision of wireless internet remains on the books as of mid-2014, putting those businesses that provide wireless access at risk of violating the law if the law is later enforced by regulators.

Fixed-line internet subscribers must first buy a landline package from Tunisie Télécom (TT), which manages the country’s 92.5 Gbps bandwidth capacity, before choosing one of 11 ISPs. Prices range from TND 10 (US$ 5) a month for a connection speed of 1 Mbps to TND 50 (US$ 27) for a connection speed of 20 Mbps. On top of this cost, subscribers must also pay for a separate ISP package, ranging from TND 10 to 25 (US$ 5 to 14). 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.

In the past, the ICT market consisted of five privately owned ISPs: Planet Tunisie, 3S Globalnet, Hexabyte, Topnet, and Tunet. However, in recent years Topnet, Tunet, and Planet Tunisie were acquired by Tunisie Télécom, Tunisiana, and Orange Tunisie Internet (OTI), respectively. In June 2013, Emirates International Telecommunications (ETI) announced its plan to sell its 35 percent stake.

---

in Tunisie Télécom, citing employees’ strikes over higher salaries as a reason for the move. In 2011, Tunisia’s interim authorities seized a 51 percent share of Orange Tunisie that was formerly held by another son-in-law of Ben Ali, Marwan Ben Mabrouk.

In addition to operating the backbone network, Tunisie Télécom has a monopoly on Tunisia’s international submarine communications cables. Consequently, all international calls and data need to transit through Tunisie Télécom’s submarine cable landing stations. There are no laws that prevent ISPs from installing their own infrastructure, but huge costs have prevented this so far. In mid-2013, Orange Tunisie and Tunisiana announced a joint plan to deploy the country’s first private undersea cable, with development expected to take two to three years.

The Ministry of Information and Communication Technologies is the main government body responsible for the ICT sector. Under Article 7 of the Telecommunications Decree and Article 5 of the Telecommunication Code, ISPs must obtain a license from the Ministry of Communication Technologies in order to deliver internet services. 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 governance body and its president are 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 the invitation, sent to independent arbitrators from civil society, to 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 agency governed by a board of trustees comprised of representatives from the main shareholder, Tunisie Télécom. The latter 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.

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 and the allocation of internet protocol (IP) addresses. Together with the INT, the ATI also


22 Following the appointment of a new government in early 2014, the ICT ministry was merged with the Ministry of Higher Education and Scientific Research


manages the “.tn” country domain. The agency also provides direct internet access to public institutions.

Limits on Content

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. There have been attempts to filter pornographic content, although these have been abated by the courts. Extremist content also poses a challenge to the state, which is grappling with threats from armed extremist groups.

In June 2013, the ATI won an appeal against the filtering of pornographic material online. The case dates back to May 2011, when a Tunis-based primary court ordered the filtering of explicit content based on a complaint lodged by three lawyers, who argued that the sites were a threat to minors and the country’s Muslim values. While the ATI lost a first appeal on that case, Tunisia’s highest appeals court, the Cassation Court, threw out the verdict in February 2012, and referred the case back to the First Court of Appeals on the grounds that the ATI lacked the technical capacity to implement the mandated filtering.

As government security forces battled armed groups, which the authorities say are linked to al-Qaeda in the Islamic Maghreb (AQIM), the Interior Ministry called for the filtering of web pages affiliated with terrorism. In an interview given to al-Chourouk newspaper in February, Interior Minister Lotfi Ben Jeddou said his ministry had repeatedly called on the ICT ministry to take down content that incites terrorism, but did not receive a response. In a televised statement, a spokesperson for the ICT ministry responded by emphasizing that the removal of any type of content can only take place upon the presentation of a court order.

Although it did not constitute government action, on May 30, 2013, the official Facebook page of...
Ansar al-Sharia Tunisia (AST) was taken down by the social networking company. This occurred two weeks after the Interior Ministry banned the group from holding its annual congress. The group has since launched a new page and accused the Interior Ministry of “hacking” its previous page.

Although the government no longer advocates censorship, several laws from the Ben Ali era continue to pose a significant threat to internet freedom, even if they are sporadically enforced. Under Article 1 of the 1997 Telecommunications Decree, ISPs remain legally liable for third-party content. Furthermore, Article 9 of the 1997 Internet Regulations requires ISPs to actively monitor and take down objectionable online content. Laws allow the government to censor internet content that is deemed obscene or threatening to public order, or is defined as “incitement to hate, violence, terrorism, and all forms of discrimination and bigoted behavior that violate the integrity and dignity of the human person, or are prejudicial to children and adolescents.” Over the past year, the judiciary continued to enforce laws that restrict free speech, such as provisions in the penal code, to prosecute bloggers and social network users (see “Violations of User Rights,” below).

Although the pervasive environment of self-censorship dissipated rapidly with the fall of Ben Ali, some online activists avoid crossing “red lines” over fears of judicial prosecution. Still, users are more open to discussing religion, the army, and other sensitive issues on the web compared to traditional media platforms.

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. Late 2013 saw the birth of LerPresse, Tunisia’s first news satire website, further enriching an increasingly diverse online media landscape. In late March 2014, the Tunisian award-winning blog Nawaat launched a local and secure whistle-blowing platform in collaboration with GlobaLeaks, an open-source whistleblowing framework. Nawaat Leaks aims to allow users to anonymously and securely blow the whistle.

The abundance of online news sources has led to some cases in which partisan interests have manipulated information. There is strong suspicion that Ennahda, the former ruling Islamist party, maintains a digital army of young activists and bloggers tasked with managing Facebook communities and disseminating partisan content as part of an “info war.” The Ennahda apparatus was particularly active during antigovernment protests that swept the country following the


36 Available in Arabic at: https://docs.google.com/file/d/0B65g_tQwlE3CenNrSDZ0N1RLcip/edit


39 See http://Lerpresse.com

40 Nawaat, “Nawaat launches a special and secure site to leak confidential documents,” nawaat.org, March 27, 2014 http://nawaat.org/portal/2014/03/27/%D9%86%D9%88%D8%A7%D8%A9-%D8%A5%D8%B9%D9%88%D8%B1-%D9%8A%D8%A7-%D9%8A%D8%AA%D8%B1%D9%8A%D8%A8-%D9%88-%D8%A7%D9%86%D8%A7-%D9%84%D8%B3%D8%AA/

41 See https://nawaat.org/portal/leaks/
assassination of opposition constituent assembly member Mohamed Brahmi on July 25, 2013. Islamist Facebook pages spread rumors of terrorism attacks, including fake news of an explosion targeting an antigovernment sit-in outside the National Constituent Assembly, in an attempt to intimidate Tunisians into leaving the protests. 42

Nevertheless, the unprecedented openness of the Tunisian internet sphere in the post-Ben Ali era has greatly diluted the influence of such content. Tunisian youth and civil society organizations have continued to use digital media for initiatives relating to political and social issues. The civil society organization al-Bawsala has continued tracking the National Constituent Assembly’s work in particular the adoption process of the new constitution. 43 The group live-tweets the assembly’s sessions and publishes detailed voting records on the platform Marsad.tn. 44

During the 2013 month of Ramadan (July to August 2013), Tunisian netizens created a crowdsourced Google map of restaurants and cafés that stayed open during the day. 45 The initiative came in response to a declaration made by Adel Almi, an ultra-conservative preacher, who stated he would seek authorization from the Interior Ministry to place surveillance cameras to film those who were not observing the holy month. 46

Throughout the year, activists continued to use the hashtag #FreeJabeur as part of a wider online campaign demanding the release of Jabeur Mejri, imprisoned over the publication of cartoons depicting the prophet Muhammad. For instance, in February 2014, the “100 drawings for Jabeur Mejri” campaign brought together artists and cartoonists from 12 countries to demand his immediate release. 47 He was released one month later, but still faces prosecution on other charges.

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,” 48 the absence of significant legal reforms continues
to hold Tunisia back. 49 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 threats to independent reporting, while several Tunisians have been charged with insulting state bodies or religious values. At the same time, the creation of a new cybercrime agency has led to fears that technology could once again be misused to perform unchecked government surveillance, potentially reversing progress in internet freedom and user rights.

On January 26, 2014, the National Constituent Assembly (NCA) overwhelmingly approved the country’s new constitution. 50 The constitution, the first to be passed since the 2011 revolution, enshrines the right to free expression, freedom of the press and the media, and bans “prior censorship.” 51 Specific articles guarantee the right to privacy and personal data protection, as well as the right to access information and communication networks. However, the text contains vague language tasking the state with “protecting sanctities” and banning “takfir” (apostasy accusations). 52 Such language could act as a constitutional restriction on internet freedom, where religious issues are currently debated more openly than in the mainstream media or on the streets.

On September 17, 2013, Tunisian journalists went on a nationwide strike, 53 accusing the government and prosecutors of ignoring the country’s reformed press code, Decree 115 of 2011. 54 The law, implemented in 2012, 55 recognizes web journalists as “professional journalists” and entitles them to the same rights and legal protections granted to print and broadcast journalists. 56 The law also abolished prison sentences for criminal defamation and, in most cases, places the burden of proof on the plaintiff.

The repressive laws of the Ben Ali regime still 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. 57 While censorship is no longer a significant issue, these laws continued to be employed to prosecute internet users.

49 Index on Censorship: “Tunisia: the long road to reform is far from over”, Indexoncensorship.org, February 12, 2014 http://www.indexoncensorship.org/2014/02/tunisia-long-road-reform-far/
54 http://www.inric.tn/D%C3%A9cret-loi2011_115Arabe.pdf
On May 29, 2013, Hakim Ghanmi was tried before a military court on charges of “undermining the reputation of the army”, “defamation of a public official,” and “disturbing others through public communication networks”. Ghanmi, a journalist and blogger, had criticized the staff of a military hospital in a blog post. Two months later, he was cleared of two of the charges, but fined TND 240 (US$ 130) for defamation. Both Ghanmi and the plaintiff have appealed. However, on March 11, 2014, the verdict was confirmed by the military court of appeals in Sfax.

In mid-August 2013, Mourad Meherzi, a cameraman for the online television station Astrolab TV, was detained for filming and posting a video which showed actor and film director Nasseredine Shili throwing an egg at then-minister of culture, Mehdi Mabrouk. Meherzi was accused of “conspiracy to commit violence against government officials” and, according to his lawyer, was placed under phone surveillance. Meherzi was freed after three weeks.

In September 2013, prisons’ union leader Walid Zarrouk was detained for a Facebook post in which he criticized Tarek Chkioua, the then-general prosecutor of the Tunis Tribunal, as well as former minister of justice Noureddine Bhiri. Zarrouk was charged with defaming a public servant, spreading information “likely to harm public order” under Article 54 of the press code, and “disrupting lives through public communication networks” under Article 86 of the telecommunication law. Zarrouk was released on October 4, 2013 pending trial.

Following a surge in politically motivated violence, including the assassination of two opposition politicians, two users were imprisoned on charges of incitement to violence in early 2014. In late January, the primary court of Tunis sentenced blogger Yassine Ayari in absentia to six months imprisonment under Articles 50 and 51 of the 2011 press code. This followed a complaint lodged by leftist politician Mondher Thabet, who Ayari mentioned in a Facebook post in which he called for the “arrest and execution” of those who served under the Ben Ali regime. Ayari, who moves between Paris and Tunis, planned to appeal the verdict.


60 Tunisia Live, “Military Court Upholds Fine Against Blogger”, tunisia-live.net, March 11, 2014 http://www.tunisia-live.net/2014/03/12/military-court-upholds-fine-against-blogger/


Imed Dghij, a member of the group, “Men for the Protection of the Revolution in Kram,” was sentenced to 14 months imprisonment over a Facebook video in which he threatened judges and police officers. The group is accused by secular parties of perpetrating political violence. “We will not die until we finish you,” Dghij said in the video addressing members of police and judges unions “loyal to the former regime.” He was convicted of “incitement to violence” and “threatening and harming others’ reputation through public communication networks.” On May 10, a court of appeals reduced Dghij’s initial sentence to three months in jail.

The authorities continue to harass citizens that have been imprisoned on speech-related offenses, targeting them with other charges after they have been released from prison. Ala Yacoubi, better known as the rapper “Weld El 15,” was initially sentenced in absentia to two years in prison in March 2013 over an anti-police video clip he published on YouTube. In the song “Boulvia Kleb,” Yacoubi describes the frustrations of Tunisian youth, calling the police “dogs” and rapping “he would like to slaughter a police officer instead of sheep at Eid al-Adha.” In a bid to reduce his sentence, Yacoubi turned himself in on June 13, only to have the original verdict confirmed. He was subsequently freed on July 4, 2013 and given a reduced six-month suspended sentence. However, only two months later, he was convicted of insulting the police during a concert performance and handed a 21-month sentence along with rapper Ahmed ben Ahmed, known as Klay BBJ. Neither of the rappers were informed of the charges, but were sentenced in absentia. Ahmed had the ruling overturned on appeal in October, whereas Yacoubi was later sentenced to four months in December 2013, after he surrendered to the authorities. Yacoubi spent two weeks in jail before his acquittal and release from jail on appeal.

Similarly, after being released from prison on March 4, 2014, Jabeur Mejri continues to face legal battles. Mejri had been sentenced to seven and a half years of prison for publishing cartoons depicting the prophet Mohammad on his Facebook page, but obtained a presidential pardon from Interim President Moncef Marzouki after completing two years of his sentence. He was, however, imprisoned again one month later and sentenced to eight months in prison for “insulting a public

---


68 Express FM, “La peine de Imed Dghij réduite de 14 à 3 mois de prison” [Imed Dghij’s prison sentence reduced from 14 to 3 months], radioexpressfm.com, May 10, 2014 http://www.radioexpressfm.com/lire/la-peine-de-imed-dghij-reduite-de-14-a-3-mois-de-prison-6974

69 See https://www.youtube.com/watch?v=6owW_Jv5ng4


servant” during an investigation in to his alleged embezzlement of funds. He stands accused of stealing TND 1,600 (US$ 870) worth of train tickets while working for the Tunisian national railway company. According to his lawyer, Mejri “lost his temper and insulted the court clerk.” His eight-month prison sentence was confirmed on appeal in May 2014. Though there are reports that he has already obtained asylum in Sweden, he is banned from leaving the country, according to his support committee.

While Mejri was pardoned for the original offense, his friend Ghazi Beji was convicted 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.

Investigative journalists also face the possibility of defamation charges for exposing government corruption, as evidenced by the case of journalist and blogger Olfa Riahi. She has faced possible fines and prison sentences in the past for her work and had a travel ban imposed on her from January to March 2013. On March 8, 2013 Riahi was charged with criminal defamation under Articles 245 and 128 of the penal code and Article 86 of the telecommunications code. In a positive sign that the authorities are not taking her work lightly, former foreign minister Rafik Abdessalem was charged with corruption in January 2014, one year after Riahi wrote an article in which she said Abdessalam misused public money by spending several nights at the luxurious Sheraton hotel in Tunis.

On May 12, police arrested blogger Azyz Amami along with his friend, photographer Sabri Ben Mlouka on marijuana possession accusations, a charge punishable between one and five years’ imprisonment in Tunisia. Amami’s arrest infuriated his supporters who accused the authorities of targeting the 31-year old for his activism against the country’s harsh drug laws and in support of

---

the relatives of protesters killed during demonstrations against the Ben Ali regime.85 Prior to his arrest, Amami launched the online campaign “I Too Set a Police Station on Fire,”86 in solidarity with protesters prosecuted for “acts of vandalism.” On May 23, a judge dismissed the case, and both Amami and Ben Mlouka were set free.87

In addition to judicial prosecution, users must also be wary of extralegal attempts to silence online activists. In August 2013, blogger Lina Ben Mhenni was placed under police protection after receiving death threats.88 The move came after the assassination of opposition deputy Mohamed Brahmi in summer 2013, a period in which a number of journalists, opposition figures, and activists critical of the then-ruling Islamist party Ennadha reported that they received death threats.

Laws that limit online anonymity also remain a concern in the post-Ben Ali era. In particular, Article 11 of the Telecommunications Decree prohibits ISPs from transmitting encrypted information without prior approval from the Minister of Communications. 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.

The creation of a new government surveillance agency has raised concerns among human rights groups. The Technical Telecommunications Agency (ATT) was established by decree n°2013-4506, issued in November 2013 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. Responsibilities for conducting internet surveillance for the purposes of law enforcement will thus be 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.89

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 controlling telecommunications traffic in the framework of the protection of personal data and civil liberties”. However, the committee is dominated by government representatives appointed from the ministries of ICT, Human Rights and Transitional Justice, Interior, National Defense, and Justice.

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.90 According to Article 5 of the decree,
the ATT’s activities are not open to public scrutiny. Critics, such as Raed Chammem of the Tunisian Pirate Party, have likened it to the NSA.\(^91\) 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. Despite fierce criticism, the ATT was established with Jamel Zenkri appointed director general in March 2014.\(^92\)

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 (known by its French acronym INPDP) to amend the country’s 2004 privacy law have not been discussed by the constituent assembly.\(^93\) Mokhtar Yahyaoui, head of the INPDP, has slammed the government for not prioritizing the amendments, which aim to ensure the body’s independence from government interference.\(^94\)

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. In October 2013, the Islamist hacker group al-Fallahas hacked the Facebook page of Samir Dilou, a member of the Ennadha political party and the then-minister for human rights, as well as the website of the Communist Workers’ Party.

---


Turkey

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>14</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>19</td>
<td>23</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>49</td>
<td>55</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 76.1 million

- Internet Penetration 2013: 46 percent
- Social Media/ICT Apps Blocked: Yes
- Political/Social Content Blocked: Yes
- Bloggers/ICT Users Arrested: Yes
- Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Access to both Twitter and YouTube were blocked prior to local elections held on March 30, 2014. After individual petitions were submitted to the Constitutional Court, it ruled that the bans violated the freedom of expression of all users and the blocking orders were subsequently overturned (see Limits on Content).

- Amendments to the controversial Law No. 5651 on regulating the internet were made in February 2014. Among many additions, the changes extend the liability of hosting and access providers, introduce one- to two-year data retention requirements on providers, establish an Association for Access Providers to centrally enforce blocking orders, and allow URL-based blocking of websites for cases involving a violation of personal rights or privacy infringements (see Limits on Content).

- Social media platforms were widely used during the Gezi Park protests in May 2013, when mainstream Turkish media failed to report on widespread civil discontent. In the aftermath, at least 30 people were detained and investigated on the basis of their tweets and other online postings (see Violations of User Rights).

- Osman Garip was sentenced to over a year in jail for defaming Prime Minister Erdogan on Facebook, while an individual with “Allah” in his Twitter handle was jailed for 15 months for offending religious values. Similarly, two staff members at a popular Turkish website were given lengthy suspended sentences for offending religion, while renowned pianist Fazil Say received a 10-month suspended sentence in a September 2013 retrial related to “offensive” tweets (see Violations of User Rights).

- A law passed in April 2014 allows the Turkish intelligence agency (MIT) to request user data from ISPs without the need for a court order, while setting out broad circumstances in which the agency may intercept communications. MIT officials were also given some degree of immunity over their actions (see Violations of User Rights).
Introduction

Mass protests, corruption scandals, and local elections contributed to a tumultuous year in Turkey. In each of these three areas, the internet has been a key battleground for control. In June 2013, protestors took to Istanbul’s Taksim Gezi Park in a bid to halt construction of a shopping mall on the site. Police responded with brute force, escalating the low level demonstrations into a broader protest against the disproportionate police violence and the government of Prime Minister Recep Tayyip Erdoğan, who in August 2014 was voted president in Turkey’s first direct elections for the post. Traditional Turkish media—much of which is owned or controlled by elements close to the ruling Justice and Development Party (AKP)—refused to cover the events, moving most coverage to online channels and social media. This led Erdoğan to label Twitter “the worst menace to society” as part of an overall strategy of demonizing and discrediting social media, one of the few forms of information that is not yet controlled by progovernment individuals. Turkey temporarily blocked Soundcloud, Vimeo, and other social media platforms during the coverage period, and in total, the amount of blocked websites increased by 11,000 to over 40,000 by April 2014.

Social media took the spotlight for a second time in December 2013. Recordings posted to YouTube, purporting to reveal illegally wiretapped conversations between top government officials, including Erdoğan, appeared to implicate many in corruption allegations. Erdoğan dismissed the tapes as distorted and characterized their circulation as part of an attempt by Fethullah Gülen, a U.S.-based exiled preacher, and his followers to take down the government. The leaks led to the dismissal or reshuffling of hundreds of police officers and judges with suspected ties to Gülen, once an ally of Erdoğan’s AKP. In February 2014, a judiciary reform law was passed to boost the influence of the Justice Ministry in appointing judges in a clear threat to judicial independence, although elements of that law were later overturned by the Constitutional Court in April.

The role of social media in the “Occupy Gezi” protests and the dissemination of leaked wiretaps led to significant movement on the legal front. Lawmakers passed amendments to Turkey’s Law 5651, which regulates the internet, in an attempt to provide a stronger legal basis for the immediate blocking of content that violates privacy—for example, leaked audio recordings—and, in exceptional cases, entire social media platforms. The amended law also placed heavy burdens on intermediaries such as ISPs and cybercafes. Protests in Taksim Square in January 2014 did not halt the passage of the bill, introduced as part of an omnibus package, in February. The law attempted to provide a sound legal basis for the blanket blocking of social media platforms, which escalated one month later.

In advance of local elections on March 30, the government took greater steps to limit the flow of information. Twitter was blocked in its entirety on March 21 for failing to comply with government requests to ban anonymous users that had posted links to alleged corruption leaks. In the ensuing

---

2. Engelliweb.com is a website that documents information about blocked websites from Turkey. Site accessed April 30, 2013.
outcry, the discovery and sharing of workarounds by tech-savvy users led to a sharp increase in the number of tweets from Turkey. This spike in activity was short-lived, however, as the regulator took steps to block alternative methods of accessing banned sites. Six days later, YouTube was blocked after the apparent leak of a recording of top national security officials debating the possibility of faking an attack on Turkey in order to justify military intervention in Syria.

The bans on Twitter and YouTube were eventually overturned on April 3 and May 29, respectively, after historic decisions from the Constitutional Court. The Turkish judiciary has served as a crucial check against executive authorities in the fight for internet freedom in the country. Supranationally, citizens have filed five separate applications to the European Court of European Rights (ECtHR) to challenge the government's past blocks. In December 2012, the court ruled in the case of Ahmet Yildirim v. Turkey, unanimously finding that the blanket blocking of entire platforms, in this case the hosting service Google Sites, violates freedom of expression provisions in Article 10 of the European Convention of Human Rights. A separate application related to the blocking of Last.fm has yet to be decided, while the ECtHR published the statement of facts for applications related to a case on YouTube on April 16, 2014. The court has asked the Turkish government to comment on the applications by September 20, 2014. Rather than take steps to remedy the country's laws on the internet, the Turkish government has only passed more laws that worsen the rights and freedoms of Turkish users. Turkish lawmakers passed a law in April to allow intelligence agents broad access to stored user data as well as greater scope for intercepting online communications without a court order, while making it more difficult for agents to be held accountable by the courts.

Turkish users also faced increased arrests and legal prosecution for their online activities. Dozens of people were charged with inciting protests or defaming the prime minister over tweets relating to the Gezi Park demonstrations. Osman Garip, a university student, was sentenced to over a year in prison for defaming Erdoğan on Facebook. Several others were ordered to pay fines on similar charges. Poet and pianist Fazil Say, as well as staff at the popular Turkish website Ekşisözlük were handed lengthy suspended sentences for offending religion, while a Twitter user with the word “Allah” in his Twitter handle was sent to jail for 15 months for the same charge. Overall, decisions to punish users or restrict content on disproportionate political, social, or religious grounds continue to imperil Turkish internet freedom.

Obstacles to Access

Despite an increasing penetration rate in the last few years, obstacles to internet access in Turkey remain. Internet penetration stood at 46.25 percent in 2013, up from 34.37 percent in 2008. As of mid-2014, the number of broadband subscribers has reached 37 million, according to Turkey's Information and Communications Authority (BTK), of which 28.4 million were mobile broadband.
subscriptions. In total, mobile penetration was at 92.96 percent in 2013 and all mobile phone operators offer third-generation (3G) data connections.

Most users access the internet from workplaces, universities, and internet cafes. 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. While prices have decreased, they do remain high. Bandwidth capping has become standard practice and a part of the broadband services offered by major providers since 2011. A lack of technical literacy, particularly among older Turks, also inhibits wider internet use.

There are around 150 internet service providers (ISPs) in Turkey, though the majority act as resellers for the partly state-owned company Turk Telecom, whose subsidiary TTNet controls around 78 percent of the broadband market. Turkcell is the leading mobile phone provider, with 48.92 percent of subscribers, followed by Vodafone and Avea. Overall, delays in the liberalization of local telephony continue to undermine competition in the fixed-line and broadband markets. ISPs are required by law to submit an application for an “activity certificate” from the Telecommunications Communication Presidency (TIB), a regulatory body, 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.

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 “.com.tr” and “.org.tr” domain names unless they own a company or civil society organization with the same name as the requested domain. A new set of rules on domain names registration was published in the Official Gazette on November 7, 2010.

The BTK and the TIB, which it oversees, act as the regulators for ICTs and are well staffed and self-financed. 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 TIB also oversees the application of the country’s website blocking law and is often criticized by pressure groups for a lack of transparency and its apparent lack of independence from the executive.

---


10 “Electronic Communications Market in Turkey – Market Data (2014 Q2),” Slide 32. Figures do not include cable internet.


Limits on Content

Internet censorship continues to increase steadily in Turkey. Over the past 12 months alone, access to around 11,000 additional websites was blocked.\(^{13}\) This figure includes numerous sites that were blocked for political or social reasons, such as news outlets or online communities that report on LGBTI issues, ethnic minorities, or events in the southeast of the country, which is home to a decades-long separatist conflict with Kurdish militants. Changes to Turkey’s internet law entrusted the TIB with broad discretion to block privacy violations, while failing to establish strong checks and balances. These changes came after the leaking of alleged phone conversations of top government officials on December 17, 2013, and laid the groundwork for the eventual blocking of social media platforms such as Twitter and YouTube. Access to WordPress, DailyMotion, SoundCloud, and video-sharing platform Vimeo was also temporarily blocked over the coverage period. Social media facilitated the dissemination of leaks, and mobilization of massive protests in Istanbul’s Taksim Gezi Park and elsewhere.

The blocking and removal of online content is regulated under the “Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication,” referred to as Law No. 5651.\(^{14}\) The law was initially established 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.\(^{15}\) 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, first passed in 2007, has already been found to be in contravention of the European Convention of Human Rights.

Blocking orders are issued by courts as well as the TIB.\(^{16}\) 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 TIB’s mandate includes executing judicial blocking orders, but it can also issue administrative orders under its own authority for certain content. Moreover, in some cases it has successfully asked content and hosting providers to remove offending items from their servers, allowing it 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 December 2011, an administrative court in Ankara rejected an appeal to obtain official blocking statistics under Turkey’s freedom of information law. A subsequent appeal to the Council of State, #44

---

\(^{13}\) Engelliweb.com is a website that documents information about blocked websites from Turkey. Site accessed April 30, 2013.


\(^{16}\) According to TIB 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 TIB. Reporters Without Borders, “Telecom Authority Accused of Concealing Blocked Website Figures,” news release, May 19, 2010, [http://en.rsf.org/turkey-telecom-authority-accused-of-19-05-2010.37511.html](http://en.rsf.org/turkey-telecom-authority-accused-of-19-05-2010.37511.html).
Turkey

the highest administrative court in Turkey, was lodged in January 2012 to obtain the statistics. The Court had not issued a decision as of May 2014.

Currently, access to a number of well-known sites and services is blocked, including Last.fm, Metacafe, the digital library Scribd, and Ktunnel, a popular proxy service that was blocked in late 2013. 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 Atilim, Özgür Gündem, Azadiya Welat, Keditör, Günlük Gazetesi, and Firat News Agency.

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 which features writings of a sexual nature, and the Playboy website. 5Posta is blocked by two different decisions, and an appeal is ongoing. An individual petition was separately lodged with the Constitutional Court by the owner of 5Posta in November 2013. Similarly, two university professors lodged an appeal at the Council of State level against the Playboy block in early 2014. Grindr, a mobile application that uses location data to connect gay, bisexual, and bi-curious men, became the first app to be rendered inaccessible from Turkey in August 2013. The Istanbul 14th Criminal Court of Peace blocked the app as a “protection measure.” The ban also covers the application’s website. Grindr had over 125,000 active monthly users at the time.

In addition to these compulsory 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. The child filter blocks access to Facebook, YouTube, Yasam Radyo (“Radio Life”), the Armenian minority newspaper Agos, and several websites advocating the theory of evolution, while 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 in 2012, but was largely made up of BTK members or appointees, and does not appear active.

The BTK tried to mandate filtering for all users in 2011, but withdrew the proposal following a legal challenge. A decision on a separate challenge to the legality of the voluntary filters launched by the Alternatif Bilişim Derneği (Alternative Information Technologies Association) in expected from the Council of State in 2014.

---

23 On September 27, 2011, the Council of State rejected the “stay of execution” request by Binanet referring to the annulment of the February 22, 2011. The case between Binanet and BTK is currently on-going as of early 2012.
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 a number of parliamentary written questions, the Ministry acknowledged that it uses Fortiguard web filtering software at primary education institutions. In a separate written response to Member of Parliament (MP) Ibrahim Binici dated February 27, 2012, the administrators of the Turkish parliament said that internet access within parliament was filtered and that access to gambling, pornographic, gaming, and terrorist websites is blocked. In December 2012, they rejected claims that access to websites pertaining to the Alevi Islamic minority was among the content blocked.

Rather than addressing Law No. 5651’s shortcomings in the wake of public criticism, one of the main legal developments over the past year in Turkey was the passage of amendments which made it more repressive. While the original version of Law No. 5651 included only notice-based liability and takedown provisions for violations of individual rights, the amended version extends this provision to include URL-based blocking orders to be issued by a judge at a Criminal Court of Peace in relation to the objectionable content. In certain circumstances, if deemed necessary a judge may also issue an order to block complete domains such as YouTube or Twitter.

The amendments expanded powers for the TIB. When the privacy of an individual or legal entity may have been violated, they can now apply directly to the TIB, who can issue an order to ISPs to block the content in question. While the TIB does not require a court order to have the content blocked, under the law, the victim of the privacy violation must submit a court petition within 24 hours. The court must then rule on the matter within 48 hours, otherwise the order is suspended and the content is unblocked. If the court decides to block the website, only then can an individual apply to a court to reverse the decision. In cases where no complaint has been received, but content may result in adverse consequences to the privacy of others, the head of the TIB can also act ex officio to block at his or her own discretion. Individuals may also dispute this in a court. The amended version of Law No. 5651 also shields TIB staff if they commit crimes during the exercise of their duties. Criminal investigations can only be initiated subject to an authorization from the TIB Director for TIB staff and from the relevant Minister for the TIB Director. This process casts a serious doubt on the functioning and accountability of the TIB.

Under the newly amended law, ISPs are required to set up a new Association for Access Providers, membership of 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 TIB within four hours under a penalty of up to TRY 300,000. Failure to take measures to block all alternative means of accessing the blocked site, such as proxy sites, may result in a fine of up to TRY 50,000 (US$ 22,000).
Turkey

The most criticized and publicized blocks imposed in the past year involved social media platforms. On December 17, 2013, links to unverified audio tapes which appeared to implicate Erdoğan, his son Bilal, and several ministers in high-level corruption, were disseminated on Twitter. The recordings, leaked during a widespread corruption investigation, led some to demand Erdoğan’s resignation. An anonymous Twitter account also released hundreds of pages of documents, allegedly from a police investigation into the corruption affair. Erdoğan blamed U.S.-based preacher Fethullah Gülen for ordering illegal wiretaps via his supporters in the police and judiciary, in a plot to bring down the government. 28

On March 20, 2014, shortly before local elections, Erdoğan vowed to “wipe out” the social network, which he referred to as “Twitter, schmiter!” 29 The next day, the TIB unilaterally issued an order to block the platform, citing Twitter’s failure to comply with three court orders and one prosecutor’s decision to ban “fake” users that defamed public officials. 30 Twitter challenged one of the blocking decisions in a local court, pointing to its status as a hosting provider and the fact that it does not hold operations within the country puts the company outside of Turkish legal jurisdiction. 31

Less than a week later, a video posted on YouTube broadcast audio of a conversation which allegedly took place between top security officials in which they discussed mounting a fake attack on Turkey in order to strengthen public support for Turkish military intervention in Syria. 32 Within hours, the entire YouTube platform became inaccessible after the TIB blocked it through a “precautionary administrative measure” based on an order from the Gölbashi Court of Peace. 33 Ahmet Davutoğlu, Turkish foreign minister at the time, said “the ban on YouTube is a matter of national security.” 34 This was not the first time that YouTube or other video-hosting sites have been blocked in the country. YouTube was intermittently blocked between 2007 and 2010 to prevent users from accessing videos critical of Turkey’s founding father Mustafa Kemal Atatürk. The Istanbul 10th Criminal Court of Peace separately issued an order to block Vimeo for 24 hours on January 9, 2014. 35 Citizen journalists had been using the site to post videos of countrywide protests. 36

---

In a momentous step, the Constitutional Court intervened on the side of freedom of expression in both cases. Two law professors, Yaman Akdeniz and Kerem Altiparmak, petitioned the court against the Twitter block, arguing that the TIB order was arbitrary and without legal basis. In April, the court ruled that the order violated the applicants' freedom of expression, safeguarded by Article 26 of the constitution and ordered the TIB to lift its blocking decision. Twitter was unblocked on April 3, after the AKP emerged victorious in the March 30 local elections.

Challenges to the YouTube ban went back and forth in local courts. The Gölbaşı Court of Peace, responsible for the initial ban, changed its ruling in April to ban 15 specific videos instead of the entire site. The higher Gölbaşı Criminal Court of First Instance overturned that decision, ruling that all of YouTube must remain blocked until it removes all “criminal content,” and the platform remained inaccessible. On May 29, the General Assembly of the Constitutional Court ruled that the ban was unconstitutional and infringed on applicants' freedom of expression. Access to YouTube was restored on June 3, more than two months after the initial ban.

In addition to widespread filtering, state authorities are proactive in requesting the deletion or removal of content online. According to the BIAnet news website, numerous news sites faced the threat of closure if they did not remove content. In one example, T24 was asked by the TIB to remove a report related to a parliamentary question posed by opposition parliamentarian Umut Oran that referenced corruption allegations related to the sale of Turkuaz Media Group, and implicated Erdoğan, his son, business connections, and other politicians. Oran, Deputy Chairman of the opposition Republican People’s Party (CHP), was also asked to remove details of his inquiry from his personal website. A court had ruled in favor of a TIB petition that the article should be removed.

Turkish government officials said Twitter had blocked access to two anonymous accounts and removed over 200 posts, after meeting with them in April 2014. The two accounts had followers of around 400,000 users each and were involved in disseminating the contested audio leaks. In its latest Transparency Report, Twitter indicates that it has received 65 court orders and 121 executive
orders from January 1 to June 30, 2014, and has complied in 30 percent of total cases.\(^\text{47}\) In the previous six-month period, Twitter received two requests to remove content from Turkish courts, with no instances of compliance.\(^\text{48}\) As of mid-2014, Twitter had refused to comply with Turkish pressure to open up a local office in order to allow “closer coordination” between the two. The move would also have significant tax implications.\(^\text{49}\)

Facebook came under fire from members of the Peace and Democracy Party (BDP), Turkey’s largest pro-Kurdish political party, for removing several pages related to the group in July and August 2013. The personal fan pages of BDP parliamentarians such as Altan Tan, Sırrı Süreya Önder, Hasip Kaplan, and Leyla Zana were deleted for allegedly violating Facebook’s terms of use on praising internationally-recognized terrorist organizations.\(^\text{50}\) BDP representatives denied that the pages contained any violent content, instead saying that Facebook had removed the pages for an interview with a BDP parliamentarian in which he called for greater autonomy for “Kurdistan.”\(^\text{51}\) Facebook also banned pages run by a number of alternative news sources, including Yükselova Haber (Yükselova News), Ötekilerin Postası (The Others’ Post), Yeni Özgür Politika (New Free Policy), Kürdi Müzik (Kurdish Music), and other groups related to Kurdish movements during 2013.\(^\text{52}\) The BDP said Facebook’s censorship policy was harsher than that of the Turkish government, on grounds that Facebook pages run by the ruling AKP include praise of Hamas, which the US and European Union have designated a terrorist organization; and that the government is in talks with the Kurdish Worker’s Party (PKK), which is also a designated terrorist organization. Facebook was separately criticized for suspending pages used by antigovernment activists.\(^\text{53}\)

Although Google has not made available any of information on government requests to remove content over the past year, Turkish media reports in March indicated that at least three YouTube accounts that had uploaded leaked audio conversations were suspended.\(^\text{54}\)

When they were available, social-networking sites were crucial for internet users mobilizing protests during the coverage period. In late May 2013, what started as a relatively small and peaceful protest over a plan to transform Gezi Park into a shopping mall rapidly descended into a series of massive demonstrations against police abuse and a disproportionate use of force from Istanbul to Ankara, İzmir, Adana, and other cities. Turkish mainstream media largely failed to report on the events; instead YouTube, Facebook, and Twitter arose as some of the few outlets for reliable coverage on


the protests, leading Prime Minister Recep Tayyip Erdoğan to describe social media as “the worst menace to society.”

Journalists and scholars who are critical of the government faced coordinated 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, counter government critics, and drive discussions on important foreign policy issues on social media. The move was seen as a response to the use of social media during the Gezi Park protests, when the far majority of Turkish Twitter users were critical of the government. AKP advisors are quick to instruct followers to retweet progovernment messages or infographics that smear opposition critics. “One has to beat them at their own game,” the mayor of Istanbul said in 2013. Some observers have speculated that the government may have hired PR companies or bought tens of thousands of fake followers as a part of the strategy. Turkish newspaper Radikal has also reported that the Gülen movement, followers of US-based Sunni Muslim cleric and former AKP ally Fethullah Gülen, have used similar tactics to protest government. Erdoğan himself has complained of a “robot lobby” of bots on social media that churn out antigovernment tweets.

Turkish users increasingly rely on internet-based publications as a primary source of news, and despite the country’s restrictive legal environment, the Turkish blogosphere is surprisingly vibrant and diverse. There are a wide range of blogs and websites through which citizens question and criticize Turkish politics and leaders, including issues that are generally viewed as politically sensitive. The majority of civil society groups maintain an online presence.

Despite the large number of websites 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, a large number of articles are published to instruct users on how to access the banned websites. YouTube was the eighth most-accessed site in Turkey in 2010, when it was widely blocked. However, when internet users employed Google’s Domain Name System (DNS) service and OpenDNS to evade blocks during the blocking of both Twitter and YouTube in 2014, Google announced that they had received several credible reports and confirmed with their own research that Turkish ISPs had intercepted the hijacked settings.

---

Protestors once again took to the streets on January 18, 2014 to protest against the rushed amendments to Law No. 5651. Hundreds gathered in Istanbul’s central Taksim Square for a peaceful rally, only to be dispersed by police using water cannons and teargas.  

Violations of User Rights

The passage of restrictive laws, mounting physical assaults on online journalists, and cyberattacks against independent news sites during critical periods contributed to an overall decline in Turkish users’ digital rights over the past year. As social media gained more prominence as a tool for activism, legal cases against Facebook and Twitter users has increased. Over the past year, well known personalities were charged with inciting protests, defaming the prime minister, insulting public authorities, or offending religious values for their posts. At the same time, intelligence agents have gained greater surveillance powers, as judicial checks on executive authorities continue to weaken.

The Turkish constitution includes broad protections for freedom of expression. Article 26 states, “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 law 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, although there are limitations on the use of encryption devices, and surveillance by security agencies is highly prevalent. There are no laws that specifically criminalize online activities like posting one’s opinions, downloading information, sending e-mail, or transmitting text messages. Instead, many provisions of the criminal code and other laws, such as the Anti-Terrorism Law, are applicable to both online and offline activity.

Dozens of Twitter users, some with only hundreds of followers, were detained for tweeting “propaganda” or “misleading information” in relation to the June 2013 Gezi protests. At least 29 individuals face up to three years in prison for tweets that called on users to join protests, often by simply providing the location of the protests. Prominent actor Mehmet Ali Alabora was called in for questioning in July 2013 after he tweeted, in the course of the Gezi Park protests, “It is not just Gezi Park, mate. Haven’t you understood it yet? Come along.” After Prime Minister Erdoğan publically complained about the tweet, Alabora was accused of “inciting an armed rebellion against the government” under Article 313/1 of the penal code, a charge that carries a prison sentence of up to 6 years.

---

to 25 years. In January 2014, the Istanbul Public Prosecutor’s Office dismissed allegations against Alabora.

Legal action is also taken against users deemed to have insulted public authorities. In November 2013, Osman Garip, a 24-year-old university student, was sentenced to 1 year and 15 days imprisonment by a Criminal Court of Peace in Konya for defaming the prime minister on Facebook during the Gezi protests. Garip has announced that he will appeal against the decision. Furthermore, the journalist Gökhan Kaya is under investigation for allegedly defaming the police forces for a tweet he posted during the Gezi protests.

Erdoğan has filed hundreds of similar defamation suits in order to silence critics. İhsan Eliaçık, the leading figure of a “Socialist Muslim” movement, faced prosecution for defaming Erdoğan on Twitter. Erdoğan’s lawyers filed a petition with a court in Ankara related to 12 tweets in June 2013. In January 2014, Eliaçık was ordered to pay civil damages of TRY 2,000 (US$ 900) related to nine tweets in which he was highly critical of Erdoğan, calling him such things as a “dictator, a corrupt leader, provocateur, liar and arrogant.”

A petition was also filed in June 2013 against Hüseyin Aygün, a member of parliament from the opposition CHP, for civil damages of TRY 100,000 (US$ 44,400) related to defamatory tweets. Aygün had called Erdoğan a “terrorist” while tweeting during the Gezi protests. He was later ordered to pay TRY 25,000 to Erdoğan.

In November 2013, Erdoğan sued two LGBTI activists for defamation related to ironic tweets they had posted about the prime minister. The tweets related to a statement by Erdoğan, a Sunni, in which he sought to boost his credentials with the country’s Alevi minority by claiming his love of Ali, an imam they revere, made him a “four out of four” Alevi (dört dörtlük, a Turkish idiom meaning “perfect” or “through and through”). Critics saw this as yet another example of Erdoğan paying
tribute to an oppressed minority in his rhetoric, while continuing to take actions that oppress them. In this context, Levent Pişkin, an LGBTI activist and District Chair for the People’s Democratic Party (HDP), tweeted, “I now expect from the PM the following statement: I’m queer (ibne) myself, four out of four, and I’m not about to learn being queer from the likes of you.” Hakan Demir, also an LGBTI activist and a blogger, posted a similar tweet. After Demir and Pişkin were charged with criminal libel, the latter subsequently countersued the prime minister for implying that being homosexual is an insult. In May 2014, Pişkin was fined TRY 1,500 (US$ 660) for defamation in a sentence that the court said was equivalent of two and a half months in jail.

Users also face arrest and prison terms for online posts that are deemed to insult or offend religious values. One of the cases that received the most media attention in recent years relates to the composer and pianist Fazil Say. In June 2012, Say was charged with offending Muslims over posts he made on Twitter, including an April 2012 tweet in which he joked about a call to prayer lasting only 22 seconds and for retweeting several lines attributed to the poet Omar Khayyam. Say was charged in June 2012 with inciting hatred and public enmity, as well as insulting “religious values” under Section 216(3) of the criminal code. He received a suspended sentence of 10 months in prison, meaning that his sentence will not come into force unless he commits another offense within five years. However, subsequent to an appeal by his lawyers to annul the sentence, a retrial was ordered in April 2013. At the retrial, the 19th Istanbul Criminal Court of Peace once again handed Say a 10-month suspended sentence in September 2013 for insulting religious values on Twitter. He must also remain under court supervision.

In another case related to blasphemy, Turkish-Armenian linguist and former columnist Sevan Nişanyan was sentenced to 13 months imprisonment in April 2013 for “publicly insulting the religious values of part of the population.” The allegations related to a blog entry he authored in 2012 about the “Innocence of Muslims” video which sparked protests across the Arab world.

---

76 LGBTI News Turkey, “We know faggotry very well!” November 21, 2013, http://lgbtinewsturkey.com/2013/11/22/levent-piskin-we-know-faggotry-very-well/.  
80 The Guardian, Turkish pianist Fazil Say on trial for ‘insulting Islam’ on Twitter, October 18, 2012 at http://www.guardian.co.uk/world/2012/oct/18/turkish-pianist-fazil-say-islam.  
Nişanyan, currently imprisoned for another unrelated crime, launched an ongoing appeal against the sentence.85

On May 29, 2014, a user with “Allah” in his Twitter handle was sentenced to 15 months in prison for offending religious values.86 The holder of the account, was accused of “writing harmful content” by pretending to write in the voice of God, at times to criticize Turkish officials.87 The user said that his account had been hacked.

In August 2013, the Public Prosecutor’s Office in Istanbul charged Sedat Kapanoglu and 40 other users with publicly degrading religious values due to their posts on Ekşisözlük (“Sour Dictionary”), a popular social media website in Turkey. Kapanoglu is the owner of the social media platform which features posts on Muslim, Christian, and religious topics, among others. In May 2014, Kapanoglu and Özgür Kuru received suspended sentences of 10 and 7.5 months, respectively. The other 38 defendants had their cases suspended.88

Several court cases in recent years have illuminated how other laws are being used to prosecute online activity. For example, in October 2011, the Anti-Terrorism Law was used to prosecute journalist Recep Okuyucu for allegedly advocating terrorist propaganda by downloading Kurdish music files and accessing the blocked Kurdish Firat News Agency website.89 A Diyarbakir court found him not guilty. More recently, Adana High Criminal Court No. 8 sentenced Metin Öztürk to nine years and seven months’ imprisonment for sharing terrorist propaganda through Facebook in January 2013.90

Ten people, including three university students, were arrested in relation to a hacking collective called Redhack which infiltrated government websites in 2012. They face terrorism-related charges, including membership in a terrorist organization.91 All denied association with Redhack, stating they do not possess the technical knowledge required to hack into government servers. Redhack says the accused individuals have no ties with the group. Indeed, speaking through social networks, Redhack stated that the terrorism allegations are simply part of the government’s ongoing targeting of its

domestic opponents. Another 14 people were detailed in November 2013, including actor Barış Atay, on accusations of links to Redhack, but released by an Ankara court after a week.

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 and buyers need to provide official identification. Turkey has yet to adopt a data protection law, though the September 2010 amendments to the Turkish Constitution included data protection provisions. It is expected that a draft data protection bill will reach the parliament during 2014. In 2011, the use of encryption hardware and software became subjected to regulations introduced by the BTK. Suppliers are now 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.

The constitution specifies that any action that could potentially 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. Despite constitutional guarantees, most forms of telecommunication continue to be tapped and intercepted. Between 2008 and 2009, several surveillance scandals received widespread media attention, and it is suspected that all communications are subject to interception by various law enforcement and security agencies, including the Gendarmerie (military police). Some reports indicate that every day, up to 50,000 phones—both mobile and landlines—are legally tapped, and 150,000 to 200,000 interception requests are made each year. During 2013 and 2014, stories related to the bugging of the prime minister and top officials continued to hit the headlines.

In April 2014, a law was passed that expanded the powers of the National Intelligence Agency (MIT). Law No. 6532 on Amending the Law on State Intelligence Services and the National Intelligence Agency allows intelligence agents unfettered access to communications data with no need for a court order. The law forces public and private bodies to hand over data, documents, and information to the MIT upon request, with failure to do so punishable by prison. In the clause relating to the ability of the MIT to intercept and store private data related to “external intelligence, national defense, terrorism, international crimes, and cybersecurity passing through telecommunication channels”, there is no requirement to procure a court order. The law also limits the ability of the judiciary or press to hold the MIT accountable for wrongdoing. Courts must acquire 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, a new provision. Some observers have commented that the bid to shield the MIT from judicial investigations was intended to provide legal cover for the agency’s ongoing negotiations with the Kurdish Workers’

Party (PKK), which is officially recognized as a terrorist organization; it also facilitated the crackdown on domestic movements such as the Gülenists.96

These surveillance practices have been challenged in court on at least one occasion. In 2008, responding to complaints lodged by the TIB, the Supreme Court of Appeals overruled a lower court's decision to grant both the Gendarmerie and the MIT the authority to view countrywide data traffic retained by service providers.97 Faced with criticism on the issue, in 2008 the parliament launched a major inquiry into illegal surveillance and interception of communications, though the inquiry concluded in January 2009 without finding any “legal deficiencies” in the interception regime. In January 2013, a new parliamentary commission was set up with a similar goal and, during its initial investigation, revealed that the Gendarmerie had intercepted the communications of 470,102 people subject to 75,478 court orders during the last 10 years.98

A Cyber Security Council was established in October 2012 and in June 2013, created a Strategy and Action Plan on Cyber Security (2013-2014). The action plan aims at identifying threats and measures to reduce or eliminate the impact of potential cyber security incidents.99

In reaction to the role of social media in the Gezi Park protests, Turkish police and intelligence authorities have stepped up monitoring of social media. In October 2013, it was reported that the Undersecretariat of Public Order and Security (KDGM) met with representatives from the police, intelligence, and the telecommunications directorate to discuss ways to prevent future mass demonstrations without resorting to blacking out 3G networks.100

While government surveillance is an issue in Turkey, ISPs are not required to monitor the information that goes through their networks, nor do they have a general obligation to seek out illegal activity. However, with the February 2014 amendments to Law No. 5651, the minimum amount of time that hosting providers must store user data was increased from 6 to 12 months, with the exact amount (up to 24 months) to be established under new bylaws that must be approved by the BTK. This also includes “Mass Use Providers,” such as cybercafes and locations that provide Wi-Fi hotspots, who must also log data on their users and abide by blocking orders. All data must be made available to the TIB upon request – and without the need for a court order – under punishment of fines of TRY 10,000 to 100,000 (US$ 4,400 to 44,000).101

98 See the Bianet article (in Turkish) at http://www.bianet.org/bianet/insan-haklari/145087-jandarma-10-yilda-470-bin-kisiyi-dinledi.
Citizen journalists and reporters for online news outlets faced physical attacks in the course of their reporting. According to Reporters Without Borders, two journalists at the news site Dokuz8Haber were attacked by police while a reporter with the BIANet news website was hit by a rubber bullet during the Gezi park protests of June 2013. A reporter for Sendika was also injured by rubber bullets in May 2014. That month, several journalists were injured or detained during May Day protests. Deniz Zerin, the publisher of the news site T24, was detained while fleeing teargas on the way to his office in Istanbul. He was not released for three days, like most of the 171 people detained during the demonstrations. Many protestors died during the demonstrations, and there has been no official investigation of police conduct.

Aside from attacks, social media users also face harassment online. Melih Gökçek, the mayor of Ankara and a member of the AKP, tweeted that local BBC journalist Selin Girit was a “traitor” and a “spy”, going so far as to create and encourage followers to use the hashtag #ingiltereadınaajanlıkyapmaselingirit (“Don’t be a spy in the name of England, Selin Girit”), according to the Committee to Protect Journalists. Supporters of the journalist created the hashtag #provokatörmelihgökçek (“Melih Gökçek is a provocateur”).

Cyberattacks against the websites of popular news organizations such as Zaman, Today’s Zaman, Cihan, Rotahaber, Radikal, Sözcü, and Taraf were recorded around the period of the March 30 local elections. Cihan, which experienced DDoS (distributed denial-of-service) attacks, speculated that the site was targeted for its reporting on election results in multiple languages. Internet access was suspended at the offices of Turkish-language Zaman and English-language Today’s Zaman for several hours.

In the past, Turkish government sites have been attacked by hacktivist organizations, such as Anonymous. During 2012, the Marxist-Socialist Redhack group infiltrated several government websites and leaked confidential information. The group has over 675,000 followers on Twitter and hacked into the servers of the Ministry of Foreign Affairs, Ministry of Finance, and the Turkish Higher Education Authority, among others, during 2012 and early 2013. At the request of a court order, Twitter made Redhack’s Twitter account inaccessible from Turkey subject to its country withhold policy during 2014.

Uganda

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>11</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>15</td>
<td>16</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>34</td>
<td>34</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 36.9 million
Internet Penetration 2013: 16 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- The Uganda Communications Act 2013 created a new media regulatory body that has been criticized for its lack of independence from the government (see Obstacles to Access).

- There were no reports of internet content being blocked or filtered during the coverage period, though an Anti-Pornography Act signed into law by the president in February 2014 threatens to hold ISPs criminally liable for the dissemination of broadly defined pornographic material (see Limits on Content).

- In response to an increasing crackdown against traditional media in the past year, critical commentary and opposition voices have become more vibrant online, leading to a palpable sense of decreasing self-censorship among some online users (see Limits on Content).

- The Anti-Homosexuality Bill, enacted in February 2014, criminalized the use of electronic devices “for the purposes of homosexuality or promoting homosexuality” (see Violations of User Rights).

- SIM card and mobile internet registrations continued through August 2013 despite concerns that the registration requirements infringe on the right to privacy given the lack of a necessary data protection law (see Violations of User Rights).

- Suspicions of proactive government surveillance of online communications increased with reports that the government had begun importing surveillance equipment and setting up internet monitoring units among the various security agencies (see Violations of User Rights).
Introduction

The internet has continued to proliferate 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 netizen community. Social media applications such as Facebook, WhatsApp, and Twitter have become significant platforms upon which Ugandans connect to each other, share information, and consume the news.

While traditional press freedom in Uganda is persistently under pressure from the government—deteriorating in 2013 due to a 10-day closure of two major media houses in May and other forms of harassment against print journalists—in general, internet freedom has not been subject to the same level of pressure or threat. There have been no reported incidents of government interference with the internet since April 2011, when the national regulator issued a directive to internet service providers (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. Instead, growing digital media activism in recent years has enabled civil society to push back on various government incursions, such as during the May 2013 shutdown of traditional media houses, which elicited widespread protests mobilized via Facebook and Twitter.

In more recent years, threats to internet freedom in Uganda have taken the form of legislative restrictions that significantly compromise access to information, freedom of expression, and rights to privacy online. In 2014, the government passed the Anti-Pornography Act, which can hold ISPs criminally liable for the dissemination of broadly defined pornographic material and require service providers to preemptively filter and block content. Another law enacted in February 2014 (but struck down in court in August), the Anti-Homosexuality Act, further threatened to restrict internet freedom by criminalizing the use of electronic devices “for the purposes of homosexuality or promoting homosexuality,” in addition to prescribing life sentences for homosexual “offenses.” LGBTI individuals were reportedly targeted for harassment on social media and attacked with technical malware throughout the year. As of fall 2014, advocates of the annulled law are working to reintroduce another version to impose the same harsh restrictions.

Meanwhile, in response to the growing threat of terrorism in the region—sparked by the 2010 Al-Shabab bombings in Kampala and heightened following the Al-Shabab gunmen siege on the Westgate mall in Nairobi, Kenya in September 2013—the government has ramped up its authority and capacity to monitor and intercept communications in the name of fighting terrorism. Reports during the coverage period documented the government’s efforts to implement voice and data surveillance of mobile phones and computers without permission from service providers. In addition, government officials spoke openly about the need to monitor social media content while also requesting a supplementary budget of US$80 million in March 2014 to procure surveillance equipment and establish a monitoring center.
Obstacles to Access

ICTs continued to expand across Uganda over the past year, resulting in increasing access to both internet and mobile phone services. In 2013, Uganda’s internet penetration rate stood at 16 percent, up from 15 percent in 2012 and just 4 percent in 2007, according to the International Telecommunication Union. Nonetheless, access to broadband internet is still rare and available mostly in urban areas, with only 0.11 percent of the population estimated to have fixed-line broadband subscriptions in 2013. Meanwhile, mobile phone penetration stood at 44 percent in 2013, a slight decrease from 45 percent in 2012. Official government statistics from the Uganda Communications Commission (UCC) reported a teledensity of 52 percent as of December 2013.

Many Ugandans access the internet at cybercafes where it costs less than US$1 for an hour of browsing. Internet access via mobile devices is becoming increasingly popular due to the growing availability of cheap mobile internet bundles. The ITU estimates that 7.4 percent of Ugandans had access to mobile broadband services in 2013. An hour of mobile web browsing (equating to approximately 20 Mb of data) costs UGX 500 (US$0.20), while a limited monthly bundle of 1 Gb costs between UGX 35,000 and 42,000 (US$12-16). Meanwhile, an unlimited mobile broadband connection can cost UGX 300,000 (US$120) for one month and over US$600 for six months. Four service providers offer their subscribers free access to Facebook.

Despite decreasing costs, internet speeds are still slow, averaging just over 1 Mbps (compared to a global average of 3.9 Mbps), according to May 2014 data from Akamai’s “State of the Internet” report. In addition, Uganda’s broadband adoption (characterized by connection speeds greater than 4 Mbps) is about 2 percent of the internet population, while the country’s narrowband adoption (connection speed below 256 kbps) is over 20 percent.

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

---

6. On the Orange Uganda network.
services. Aside from the state-owned Uganda Electricity Transmission Company Ltd, which is a licensed public infrastructure provider that has part ownership of Uganda Telecom, all the licensed service providers are privately owned entities.

In March 2014, Smart Telecom launched in Uganda, joining a competitive market dominated by bigger, well-established telecommunications brands, such as MTN Uganda, Uganda Telecom, Airtel, and Orange Uganda. Three 4G LTE network services were deployed in mid-2013. The quality of both voice and data services improved during 2014, but rumors of a possible exit by Orange Uganda from the Uganda market and leadership wrangles within Uganda Telecom in 2014 created insecurities among subscribers to these networks.

While increasing market competition has continued to drive down internet access rates, particularly on mobile phones, the cost of internet-enabled devices is US$80 on average, which is still high for the majority of Ugandans, whose median annual per-capita income is US$296 and median annual household income is US$1,775 (or US$148 per month), according to a 2013 Gallup poll on worldwide incomes. The latest 2012/13 national household survey from the Uganda Bureau of Statistics reports an average monthly household income of UGX 223,000 (US$85).

Most recently in 2013, the government launched an effort to curb the importation of counterfeit mobile phones, which may further limit access to mobile technologies. All inactive fake phones with pre-existing subscriptions were disconnected as of July 1, 2013. There are no figures to indicate how many users were affected by this initiative, but it is conceivable that the number was in the millions. In addition, a 2009 government ban on the importation of used computers remains in place.

Another impediment to increased internet usage is limited access to electricity. The national electricity distributor reports a customer base of just 458,000, most of whom are located in urban

---

areas, and alternative power sources, such as fuel-powered generators and solar energy, are very costly. Furthermore, with only about 15 percent of Ugandans living in urban areas, the divide between rural and urban access to the internet is very high due to low literacy rates, including computer literacy.

Uganda’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. Connection to these cables has led to an exponential growth in Uganda’s international bandwidth, which has decreased the costs of internet access alongside an increasing demand for data services and high speed internet. Service disruptions and slow internet speeds are still common, however, due to frequent repairs.

Over the past few years, the government has embarked on initiatives to improve rural connectivity, and a national ICT policy was finalized in 2010 to facilitate the proliferation of ICTs across the country in both rural and urban areas. Nonetheless, the national ICT sector budget allocation comprises less than one percent of the national budget. Since 2007, Uganda’s ICT ministry has been developing the National Data Transmission Backbone Infrastructure, which aims to ensure the availability of high bandwidth data connection in all major towns at reasonable prices. The project, now under the provision of the National Information Technology Authority (NITA-U), involves the installation of over 1,536 kilometers of fiber-optic cable and related equipment. As of April 2014, roughly 1,400 kilometers had been installed to connect 22 district headquarters.

The government, through the Rural Communications Development Fund (RCDF), also 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.\textsuperscript{30} 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 early 2014, 708 school ICT laboratories had been established.\textsuperscript{31}

The Uganda Communications Commission (UCC), Uganda’s telecommunications sector regulator, 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.\textsuperscript{32} 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. In addition, the UCC’s current executive director has been regarded as overzealous in his efforts to police and rein in operators, illustrating how the personal character of the regulatory authority’s leadership can in large measure determine its activities and regulations.

The Uganda Communications Act, 2013,\textsuperscript{33} which was passed by parliament in September 2012\textsuperscript{34} and signed by the president in December 2012, consolidated the provisions of the 1996 Electronic Media Act and 2000 Uganda Communications Act, and merged the old UCC and Uganda Broadcasting Council into a new Uganda Communications Commission. The new regulatory body has been criticized for its lack of independence from the government. In particular, the law places disproportionate power in the hands of the ICT minister, who 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. While the new law provides for the creation of the Uganda Communications Tribunal, which is an appeals body with powers of the High Court, its membership and advisors are appointed by the president and ICT minister.

\begin{enumerate}
\item \textsuperscript{30} Uganda Communications Commission, “Rural Communications Development Policy for Uganda,” January 2009, \url{http://www.researchictafrica.net/countries/uganda/Uganda%20Rural%20Communication%202009.pdf}.
\item \textsuperscript{32} Uganda Communications Commission, “UCC Licensing Regime,” accessed July 31, 2013, \url{http://www.ucc.co.ug/data/qmenu/11/Licensing.html}. Pursuant to the telecommunications (licensing) regulations 2005, UCC issues two types of licences: Public Service Provider (PSP) and Public Infrastructure Provider (PIP). The application fee for both license types is $2,500 dollars (a PIP license requires a one-off initial fee of $100,000), and annual fees range from $3,000-$10,000. These licenses allow holders to either set up telecommunications infrastructure or provide telecommunications services. The UCC levies a 1 percent charge on providers’ annual revenue.
\end{enumerate}
**Limits on Content**

There were no reported incidents of government interference with the internet during the coverage period. In response to an increasing crackdown against traditional media in the past year, critical commentary and opposition voices have become more vibrant online, leading to a palpable sense of decreasing self-censorship among some online users.

To date, there have also been no known instances of takedown notices issued for the removal of online content, as well as no problematic issues of intermediary liability for service or content providers, though a new Anti-Pornography Law enacted in February 2014 will hold service providers criminally liable for vaguely defined pornographic content (see “Violations of User Rights”).

Social media and blogging platforms are freely available in Uganda, with Facebook, Twitter, LinkedIn, YouTube, and Blogger ranking among the top 15 websites in the country, according to the web analytics company Alexa. The government has continued to embrace social media platforms as a channel for public engagement, as illustrated by Uganda’s Prime Minister, Amama Mbabazi, who interacts with citizens on Twitter using the hashtag #AskthePM. In November 2013, the government developed social media guidelines to assist government agencies in improving citizen engagement online.

Further, the Google Uganda domain is available in five local languages, making the popular browser available to over seven million Ugandan internet users. However, news websites provided by Vision Group, a media company that is partly owned by the government, are only available in three local languages (out of 40 languages and 56 native dialects). The web versions of the newspapers include Bukedde, Etop and Orumuri. Other news sites of major privately owned newspapers are only accessible in English, which is not widely spoken across Uganda. Moreover, the diversity of online content and the economic viability of independent outlets are constrained by advertising revenue from both government and private sources, which is generally withheld from news outlets that publish critical content.

Routine threats from the government—such as recent shut downs of media houses perceived to be too critical of the government and reports of 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, issues of oil, land-grabbing, and presidential terms. In response to the increasing crackdown against traditional media in the past year, however, critical commentary and opposition voices have become more vibrant online, leading to a palpable sense of decreasing self-

---

censorship among some internet users. According to a small survey of internet users in Uganda from December 2013, 77 percent of respondents noted feeling free and safe to express themselves online, with some threats from state agents reported.\textsuperscript{42}

While there is no evidence of government efforts to influence or manipulate online content, there have been increasing indications that the government seeks to proactively monitor online discussions. In May 2013, for example, Cabinet Minister of Security Mulira Mukasa announced intentions to set up a social media monitoring center with the aim of monitoring social media users’ behavior in Uganda, stating that the center would target “social media users who are bent to cause a security threat to the nation.”\textsuperscript{43} There are some reports that such monitoring units already exist within various government agencies tasked with the responsibility of conducting online surveillance (see “Violations of User Rights”).

Nonetheless, 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 diversity of civil society groups are increasingly using SMS platforms and social media for advocacy and to call for protests. Additionally, blogging is continuing to rise among young Ugandans who are boldly using the internet to push the boundaries on controversial issues such as good governance and corruption.\textsuperscript{44} For example, the passage of the controversial Anti-Homosexuality Act in February 2014 drew vehement online criticism from human rights activists who vowed to challenge the law at the constitutional court.\textsuperscript{45}

Digital media activism also played a significant role in condemning the police shutdown of several print media houses for their reports on a classified government letter in May 2013, which allegedly contained the succession plans of the Ugandan president.\textsuperscript{46} Using the Twitter hashtags, #Monitorsiege, #RedPepperSiege, and #MediaSiege, journalists and media activists were able to draw widespread attention to the government's infringements on press freedom, placing unprecedented pressure on the government to respond.\textsuperscript{47} The media houses were reopened 10 days later on May 30, 2014.

Violations of User Rights

The Anti-Homosexuality Bill, enacted in February 2014, criminalized the use of electronic devices “for the purposes of homosexuality or promoting homosexuality.” SIM card and mobile internet registrations continued through mid-2013 amid concerns that the registration requirements infringe on the right to privacy given the lack of a necessary data protection law. Suspicions of proactive government surveillance of online communications were strengthened in the past year with reports that the government had begun importing surveillance equipment and setting up internet monitoring units among the various security agencies.

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, the Anti-Terrorism Act, and sections of the Penal Code—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 2002 Anti-Terrorism Act criminalizes the publication and dissemination of content that promotes terrorism, vaguely defined, and guilty convictions can carry the death sentence.\(^\text{48}\) 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.

Persistent government efforts to criminalize homosexuality in Uganda further threaten to restrict internet freedom. In February, the president signed the 2014 Anti-Homosexuality Act, which prescribed up to life imprisonment for committing the “offense of homosexuality,” putting the lives of countless Ugandan LGBTI individuals at risk of discrimination, persecution, and violence.\(^\text{49}\) Pertinent to internet freedom, article 13 of the law criminalized the use of electronic devices, which include “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.\(^\text{50}\) In a positive step, a judicial ruling struck down the law in August 2014 (after this report’s coverage period) based on an administrative technicality; the technicality, however, gives the law’s ardent advocates the ability to reintroduce the law, which they reportedly intend to do.\(^\text{51}\)

Also in February 2014, the president signed the Anti-Pornography Act, which threatens to hold ISPs criminally liable for uploading or downloading vaguely defined pornographic material on their


systems, \(^{52}\) 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. \(^{53}\) No intermediaries were prosecuted under the new law during the coverage period.

In response to growing concerns over infringements on users’ right to privacy in Uganda, civil society pushed for the passage of data protection legislation, \(^{54}\) leading the government to state intentions to draft a bill in 2014. \(^{55}\) According to the information minister, the proposed bill will "give effect to Article 27 (2) of the Constitution" \(^{56}\) and ensure that the rights of individuals during data collection and processing are upheld against the threats and attacks capable of compromising the rights of information. \(^{57}\)

In the meantime, the Ugandan judiciary has been known to rule progressively in cases involving press freedom and freedom of expression. In 2004, for example, the Supreme Court struck down a Penal Code provision that criminalized the publication of false news, and in 2010, the Constitutional Court quashed the law on sedition. While judicial rulings protecting constitutional guarantees for free expression have not prevented the government from taking action against fundamental rights, prosecutions against journalists and citizens for online expression remain rare. There were no reports of online users or journalists being detained or prosecuted during the coverage period.

In general, 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 terrorist threat in the region. 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. \(^{58}\) Not surprisingly, Uganda was among the five African countries between July and December 2013 that sent a request to Facebook seeking details on one of its users. The single request was filed under the category of "cybercrime" and was ultimately turned down by Facebook. \(^{59}\)

---


56 Constitution of Uganda Article 27 (2) states: “No person shall be subjected to interference with the of that person’s home, correspondence, communication or other property.”


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. The deadline to register existing SIM cards was extended to August 2013, after which point unregistered cards were deactivated. 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.

The 2010 Regulation of Interception of Communication (RIC) Act, which was hurriedly passed by parliament following the July 2010 Al Shabab terrorist attack in Kampala, requires telecommunication companies to install equipment that enables real-time electronic surveillance of suspected terrorists. The RIC also gives the government permission to tap into personal communications based on national security concerns, which can be requested by the security minister and granted after an order by a High Court judge. Telecommunications 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 related to national security, national economic interests, and public safety. Failure to comply with the provisions in the RIC 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) to procure surveillance equipment and establish a monitoring center in accordance with the RIC Act.

Meanwhile, telecom industry observers have noted that vibrant competition between service providers makes them to hand over information to the government requires providers without going through legal channels, though the observers also do not rule out the possibility that some companies may cooperate quietly with government requests. The research and advocacy organization, Unwanted Witness Uganda, contends that providers “have faced 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.” The security minister

---

63 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 Section 5 of the Regulation of Interception of Communications Act, 2010; http://www.ulii.org/content/regulation-interception-communications-act-2010.
64 The Regulation of Interception of Communications Act, 2010; Section 8.
65 Ibid. 71.
denied these allegations, claiming 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.68

A local news report published in December 2013 documented allegations from civil society that the government had partnered with two foreign firms for assistance with voice and data surveillance of mobile phones and computers without permission from service providers.69 According to the report's source, the surveillance activity is facilitated through malware sent to individual citizens' computers and phones, which can track user activity. Though no further details have surfaced as of mid-2014, the alleged development may indicate that the government has acquired sophisticated spyware technology such as FinSpy, which has recently been discovered in a few other African countries, including Nigeria and Ethiopia.

Additionally, a January 2014 research report indicated that the government had begun importing surveillance equipment and setting up internet monitoring units among various security agencies.70 According to the report, the State House in Entebbe has a counter intelligence desk with the primary responsibility of monitoring social media and has allegedly imported technology from China that allows the desk to simultaneously monitor ten phone calls at a time. The government has not confirmed the procurement of this technology.

Further, a Cyber Crimes Unit established in early 2014 by the Uganda Police Force to fight malicious technical attacks71 was criticized by observers as an effort to "scare off online expression given the shifting trends from the use of traditional media to online."72 According to research by Unwanted Witness Uganda, the unit had profiled "dozens of internet users particularly those deemed to be opponents of the government" in the past year,73 which is a worrisome trend as the country gears up for general elections in 2016. The government did not respond to these allegations.

In addition to potential widespread surveillance, journalists in the traditional media face a high degree of harassment and occasional violence for their reporting in print news outlets. In May 2013, journalists and media activists protesting the government shutdown of several print media houses were beaten and arrested.74 These types of violations are slowly beginning to seep into the online sphere. LGBTI activists, in particular, reported increasing harassment, both offline and online, with the passage of the Anti-Homosexuality Act in February 2014, with hate messages pervading targets'
walls on Facebook. Meanwhile, hacking attacks are also a growing concern in Uganda. In April 2014, numerous members of the LGBTI community in Uganda reported receiving email spyware known as “Zeus malware” that sought to access the contact details and confidential information from a compromised computer.

Ugandan government websites are also frequent targets of attacks coming from actors outside the country. For example, in May 2013, over 40 government websites were hacked by a group known as the “Islamic Ghosts Team” for unknown reasons. In January 2014, reports emerged that security agencies in the United States and United Kingdom had remotely hacked into the Uganda Telecom network to access data and conversations of high profile individuals in Uganda.


Ukraine

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partly 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>7</td>
<td>8</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>14</td>
<td>17</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>28</td>
<td>33</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 45.5 million

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Penetration 2013:</td>
<td>42 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 2014 Status:</td>
<td>Partly Free</td>
</tr>
</tbody>
</table>

Key Developments: May 2013 – May 2014

- In the run-up to planned elections in 2015, media ownership was consolidated in progovernment hands, and there was an increase in pressure on mainstream journalists to self-censor. However, during this time there was also an increase in the use of ICTs for political mobilization, particularly during the Euromaidan protests (see Limits on Content).

- Over 150 journalists, including online journalists and bloggers, were beaten, shot at, kidnapped, or otherwise assaulted during the Euromaidan protests (see Violations of User Rights).

- New evidence revealed the extent to which the Yanukovych administration had been conducting surveillance on online activists, journalists, and opposition leaders during the coverage period (see Violations of User Rights).

- DDoS attacks occurred against independent media websites and protest communities on social media during the protests (see Violations of User Rights).
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 May 2013 through May 2014. Due to the ongoing crises in the region, events in Crimea during this time may be excluded from this report.

Introduction

During 2013-2014, the online sphere in Ukraine faced increasing pressure, though it remained the freest part of the media landscape. The Euromaidan protests, which erupted in November 2013 in response to then-president Viktor Yanukovych’s refusal to sign an association agreement with the European Union (EU), grew into a long-term anti-government stand-off, which lasted until the end of February 2014 when the president was ousted and a new government was formed. This period was characterized by a great uptick in civic activity online and the widespread use of internet and social networks for mobilization, grassroots organizing, and coordinating information flows to Ukrainians and those abroad.

In response, this mobilization was met with significant pushback in the form of repressive laws passed by the parliament in January 2014 under pressure from the Yanukovych government aimed at curbing the protest activity along with establishing more control over independent media and the online sphere. Pressure was also exerted on journalists, activists and bloggers, who suffered physical harm, DDoS attacks, and raids on media offices, along with partial website blocking and threatening mass mobile messages. The repressive laws were rolled back at the end of January under pressure from the opposition and protesters, but tension continued under the threat of Russian invasion, as internet access was temporarily cut off in Crimea and local activists were challenged by pro-Russian forces. Ukrainian media faced DDoS attacks and massive information wars, including through the use of bots on social media and in commenting sections, as well as through propaganda and misinformation from the Russian government and Russian media outlets.

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 election monitoring, government oversight, and investigating bribery and corruption of former (or current) officials. Political parties and the new government became much more active online during the protest period, and are becoming savvier in using the tools accountably in their everyday work. The internet is also 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.
Obstacles to 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 nearly 42 percent in 2013, compared to 35 percent in 2012 and 11 percent in 2008.1 At the same time, statistics from InMind show that 19.7 million Ukrainians over the age of 15 use the internet regularly, which is close to 50 percent of all Ukrainian adults.2 For fixed-broadband subscriptions, the penetration rate was approximately 8 percent in 2012, while mobile broadband had a penetration rate of just over 5 percent.3 Meanwhile, according to Akamai, the average broadband connection speed in Ukraine was 7.6 Mbps in the third quarter of 2013 (compared to 4.5 Mbps in the same quarter of 2012),4 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$8–12), while the average monthly wage in the country was UAH 3,619 (US$360) in December 2013.5

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 around 18 percent.6 The level of infrastructure differs between urban and rural areas, contributing to an urban-rural divide in the number of users. 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 continued to grow, reaching 132 percent in 2012.7 Use of mobile internet is gaining in popularity, and an estimated 14 percent of Ukrainian mobile subscribers own smartphones.8 Cost continues to be the main barrier to higher mobile internet use. Mobile operators are still waiting for access to the military’s share of third-generation (3G) mobile phone frequencies, which the newly formed government has promised will be converted and made available to providers by the end of 2014.9 The only commercial 3G license was previously owned by formerly state-run Ukrtelecom, which was privatized in March 2011. Its 3G division, Trimob, is a separate

---

2 InMind, В Украине почти 20 млн пользователей интернета [Ukraine has almost 20 million Internet users], AIN.UA, October 24, 2012, http://ain.ua/2012/10/24/99561.
6 Tymur Vorona, В 2013 году аудитория уанета выросла на 1,5 млн и составила 17,5 млн человек — исследование [In 2013, UaNet Audience Grew by 1.5 Million And Is Now 17.5 Million People – Study], AIN.UA, February 21, 2014, http://ain.ua/2014/02/21/513820.
8 Olga Karpenko, “Смартфоны есть у 14% украинских абонентов, устройств Android втрое больше, чем iPhone” [14% of Ukrainian subscribers own smartphones, Android’s share three times that of iPhone], AIN.UA, February 20, 2013, http://ain.ua/2013/02/20/113303.
company with only about 1 million subscribers and is still reported to be looking for a buyer, leaving the issue of broader frequency conversion stalled.  

Any jamming or blocking that occurred during the protests was limited and seemed to be aimed at obstructing the work of independent media. For instance, in December 2013, journalists livestreaming and using the internet to report from a key government meeting after the first major violence at Euromaidan found their internet and mobile signals jammed. Users also reported that certain independent media sites were blocked at their companies or offices.

On January 22, social media users and some mass media outlets reported that a letter (purportedly from the Yanukovych government) was circulated to ISPs around the country warning them to prepare for a temporary shutdown of internet exchanges, wireless access points, mobile cell towers, TV and radio channels, and fixed communication lines. The Internet Association of Ukraine published a statement the next day debunking the rumors and saying the letter was a myth based on reports that the government planned to announce a state of emergency in the country. On February 28, 2013, Ukrtelecom, the country’s largest telecom provider, suffered a major outage in its phone and internet services in Crimea, allegedly after unidentified persons seized telecommunications nodes and destroyed cables. The internet monitoring firm Renesys reported registering a five-hour disruption affecting Ukrtelecom that Friday night, but noted that other ISPs serving Crimea were unaffected.

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.

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. 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.¹⁷ 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, are also starting to provide broadband internet access.¹⁸ There are about 400 ISPs in Ukraine, according to the National Commission on Communications and Informatization.¹⁹ 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, Ukernet, and Itelsat. With the exception of Infocom-SK,²⁰ all these companies are private.²¹ 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 players hold 94.6 percent of the mobile communications market.²²

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.

The ICT sector is regulated by the National Commission on Communications and Informatization (NCCIR). Members of the NCCIR are appointed by the president of Ukraine.²³ 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. For instance, in July 2011 the NCCIR (then the NCCR)

¹⁸ “Количество пользователей широкополосного доступа в Украине достигло 5,6 млн” [Number Of Broadband Internet Users in Ukraine Reaches 5.6 Million], AIN.UA, December 16, 2011, http://ain.ua/2011/12/16/68574.
refused to prolong the operating license of mobile provider Kyivstar for GSM 900/1800 frequencies.\footnote{НКРС отказалась продлевать «Киевстар» лицензию на мобильную связь} Furthermore, the 2003 Law on Communications does not guarantee the independence of the NCCIR.

A new parliamentary committee on informatization and information technologies was created in December 2012,\footnote{Верховная Рада Украины прийняла Постанову “Про комітети Верховної Ради України сьомого скликання”} ostensibly to promote the president’s promise of further development of the Ukrainian ICT market.\footnote{Ольга Карпенко, “В парламенте появился комитет, отвечающий за IT-отрасль”} So far, the committee has not made any significant decisions relating to the ICT industry.

**Limits on Content**

The Euromaidan protests did not cause the government to block or filter websites, but the short-lived anti-protest laws and extra-legal pressure on media and citizens created an atmosphere of fear, leading to self-censorship in state-controlled media. At the same time, there was a significant increase in information about the unrest provided by citizen journalists, activists, and those on the ground who uploaded or streamed videos of the protests. The subsequent Crimean crisis 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.

In January 2014, Yanukovych’s administration and the parliament violated voting procedures to pass a set of harsh anti-protest laws, which included measures limiting internet freedoms.\footnote{Український парламент проголосував за законопроєкт про обмеження вільності інформації у власному виконанні} One of the main laws, #3879, criminalized dissemination of “extremist information” and slander, including online, punishable by fines or in some cases imprisonment. The law also empowered the authorities to block a website without a court order should a violation occur, introduced tighter regulations for online news agencies (requiring them to have a license with the state), and defined human rights NGOs that receive international funding as “foreign agents,” measures that effectively restricted freedom of expression and assembly.\footnote{Україна підписала угоду про звільнення від плати за розслідування (Україна committs to unconditional pardon)} The anti-protest laws caused widespread indignation. Under growing pressure from the protesters, the opposition, and the international community,
the parliament voted at the end of January 2014 to repeal most of the laws by passing a bill that
pronounced them obsolete, which the president then formally approved.

During the Euromaidan protests, occasional blocking of certain websites was reported, but these
were mostly limited to private networks: for example, many users reported that Kyiv Boryspil airport
had blocked key independent Ukrainian media websites on its network in December 2013.

There is no current regulatory framework for systematic censorship of content online, although
there have been attempts at creating legislation which could censor or limit content. Many of these
initiatives present 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, cyberscams, 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 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.

Attempts to manipulate the online news landscape became numerous in the pre-election season
and peaked during the protests, as progovernment forces struggled to contain the information
sphere. Oligarchs close to the ruling Party of Regions, such as Sergey Kurchenko, acquired significant
media resources during the summer and fall of 2013. Kurchenko alone purchased Ukrainian Media
Holding and other assets, appointing new management in key media, which resulted in journalists
of outlets like Forbes (Forbes.ua) and Korrespondent.net resigning en masse, citing censorship and
editorial pressure. Still, online media remain varied and represent many opinions on the political
spectrum, with a key cluster of independent media playing the role of watchdogs and conducting
investigative journalism. Reputable news sites like Ukrainska Pravda and Liga.net played a key role in
the coverage of the Euromaidan protests, along with new online TV and streaming video initiatives
such as Hromadske TV, SpilnoTV, EspressoTV. Access to international media websites remained
unfettered.

The Crimean crisis led to Russian TV channels being blocked in mainland Ukraine and Ukrainian
TV channels being blocked in Crimea after its annexation, but access to online content remained
largely unaffected by these events, as most of the restrictions were physical (journalists prevented
from entering and reporting in Crimea, activists kidnapped, etc.). Activists tried to counteract the

status/4116999625678848.
31 Olga Karpenko, “За компьютерные преступления депутаты предлагают сажать на 3 года” [MPs suggest jail sentences
32 “НКРЗІ пропонує зміни до Закону України “Про Основні засади розвитку інформаційного суспільства в Україні на
2007-2015 роки”” [NCCIR proposes changes to the Law of Ukraine “On the main foundations of development of information
society in Ukraine for 2007–2015”], National Commission on Communications and Informatization official website, August 9,
33 Мультимільйонер Сергій Курченко викупив крупніші українські інтернет-порталы [Multimillionaire Sergey
34 Звільнилися 14 журналістів українського Forbes [14 Journalists of Ukrainian Forbes Resign], Ukrainska Pravda, November
information vacuum in the traditional media by setting up information networks online like Krym_SOS (Crimea_SOS) on Facebook and VKontakte to supply the latest information from the region. There were some instances of online manipulation by progovernment (and later, pro-Russian) forces, such as bots or paid commenters, and banner ads on news websites and social networks. Another form of manipulation was fake websites set up to look like popular news sites (e.g., clones of Ukrainska Pravda) that posted biased or manipulative information.

YouTube, Facebook, Twitter, and blog-hosting services such as Wordpress and LiveJournal are freely available and gained significantly more users during the Euromaidan protests. In view of the planned 2015 elections, and later during the protests, politicians, especially those in the opposition, used social media widely to publicize their ideas and express support for the protests. Many ministers in the new interim government used Facebook and Twitter to report regularly on their actions, and some activists have noted that they do respond to comments and take into account public opinion in their work, helping to increase accountability. Social networks are also used widely by activists to spread information about current events to the world, with many English-language accounts and translation initiatives springing up during the Euromaidan protests. 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. Nearly 230,000 new users joined Facebook in Ukraine during the first two months of 2014, at the height of the protests. Twitter use in Ukraine also grew, with 500,000 Ukrainians visiting Twitter per day in January 2014. In February and March 2014, daily traffic from social media sites to Ukrainian news media sites was 8 to 10 times higher than that in October 2013, demonstrating significantly higher user engagement during the months of the protests.

35 Krym_SOS on Facebook, accessed on April 15, 2014 https://www.facebook.com/KRYM.SOS.  
40 Каких украинских министров можно читать в Facebook [Which Ukrainian Ministers You Can Follow on Facebook], AIN.ua, March 17, 2014, http://aiu.in.ua/2014/03/17/516042.  
Ukrainian bloggers, journalists, NGOs, and citizen activists created a number of grassroots initiatives around the Euromaidan protests and later during the developing conflict with Russia. In addition to livestreaming video and conducting translations, social media users organized online initiatives to manage different facets of the protests, from providing for the needs of protesters to fundraising for medical aid for the injured. Other crowdsourced initiatives invited users to submit evidence of police brutality and identify riot police and thugs who participated in the violence. Activists also created crowdsourced maps of the spreading unrest in Ukraine after the most violent days of the protests, when dozens of protesters and several police were shot.

Journalists worked tirelessly during the Euromaidan period as well, most notably creating a “YanukovychLeaks” website to document and publicize the financial records found in Yanukovych’s estate after he fled the country. 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.

**Violations of User Rights**

The security of journalists and online users deteriorated in the run-up to the planned 2015 elections, and during the Euromaidan protests, journalists and bloggers faced extreme intimidation and physical violence as they were explicitly targeted for their work. Additionally, independent media and civic initiatives online faced multiple DDoS attacks during the protest period, while protesters received threatening mass text messages.

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 during the Euromaidan protests in the fall of 2013 through the winter of 2014. In addition, Article 171 of the criminal code provides fines and detention sentences for obstructing journalists’ activity. The Ukrainian judiciary, however, is prone to the same level of corruption evident in other branches of power. Many businesses, including media companies, often resort to bribes to influence the consideration of their affairs in the courts.

In 2011, online journalists achieved similar status and privileges as traditional journalists, such as the ability to obtain accreditation for parliamentary sessions and other official meetings frequented by...
the press. Nevertheless, there has been an ongoing discussion about the need for online media to register with the government. Some suggest that registration would provide additional mechanisms for protecting journalists, while others refute this idea, considering any form of registration to be an impediment to press and internet freedom.51

One of the January 2014 anti-protest laws, #3879, introduced fines for libel and prison sentences for "extremist content" without providing a clear definition of this concept.52 It also made gathering and disseminating personal information (including names and photos) about judges, police officers, and members of the special forces punishable by up to three years in prison, effectively putting a damper on independent media investigations. In a positive step, the law was repealed on January 28, less than two weeks after it was passed.

In February 2014, the Simferopol court in Crimea sentenced an IT-specialist and PR manager to a four-year suspended sentence for allegedly blocking access to the Party of Regions regional website and circulating a fake appeal from the head of the Crimean office of the party online.53 Additionally, in March 2014, the Security Service of Ukraine, acting within the new interim government, started a criminal investigation against three Ukrainian VKontakte users on charges of calling for separatism online (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).54 In accordance with a court warrant, the apartments of the three Dnipropetrovsk citizens were searched and their computers taken away. As of May 2014, the investigation was still ongoing.

There is no obligatory registration for either internet users or mobile phone subscribers at present, although the anti-protest legislation that was briefly introduced by parliament in January 2014 included a bill that would require buyers to present a passport before purchasing prepaid mobile services.55 Nevertheless, the pervasiveness of extralegal surveillance of Ukrainian users’ activities is unclear.

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 pressures 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 National Commission on Communications and Informatization 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.” Some human rights groups and internet associations are concerned that this step will aid the Security Services and the government in restricting internet freedoms by creating additional means of pressure that the government can exert over ISPs.

After former president Yanukovych fled Kyiv in late February 2014, journalists discovered extensive evidence of targeted surveillance of media and civil society actors among the documents left at his residence. The evidence included reports on users making critical statements, monitoring of protest-related posts on social media, and blacklists of key independent journalists and activists, including those from opposition and anti-corruption groups.

In an Orwellian move likely meant to intimidate the protesters out on the streets, on January 20, citizens on European Square in the center of the Euromaidan protests received a mass text message reading, “Dear subscriber, you are registered as a participant in a mass disturbance.” Reports suggested that the Ukrainian government used a tactic known as “cell tower dumps” to pinpoint the locations of cell phones in use near clashes between riot police officers and protesters. The cellphone companies denied involvement; however, it later became public that in another incident, a city court had ordered Kyivstar to disclose to the government the cell phones that were active in the area of an antigovernment protest on January 10, outside of the courthouse.

In July 2013, police searched the apartment of an online journalist from the Zhytomyr region who was investigating illegal raids on a local factory. During the raid the police took his laptop and flash drive without a court order. The journalist, Anatoly Lazarenko, said the police also threatened him with criminal prosecution.

Physical attacks against online journalists and activists escalated sharply during the Euromaidan protests, during which people who were identifiably reporting on or live-broadcasting the protests were explicitly targeted by police and progovernment thugs for their work. Tetyana Chornovil, an investigative journalist and blogger with Ukrainskaya Pravda, who was known for her investigations into corruption, faced death threats.

---

of Yanukovych and other oligarchs close to him, was dragged from her car and badly beaten in Kiev in December 2013. Well-known blogger and civic activist Ihor Lutsenko was kidnapped by progovernment forces, beaten and left for dead in a forest, but survived. Overall, during the months of Euromaidan, the Institute of Mass Information recorded over 150 cases of journalists and bloggers being beaten, shot at, kidnapped, or otherwise assaulted during the Euromaidan protests.

The confrontation with Russian forces in Crimea brought a fresh wave of intimidation against online activists and journalists, with several reports of kidnappings, threats, and physical violence. On March 9, two journalists and a spokeswoman for Automaidan – a group of motorists supporting the Euromaidan protests – went missing as they attempted to enter Crimea. Independent blogger Oleksandra Ryazantseva, together with Olena Maksymenko, a reporter with the Ukrainian Week, and Automaidan’s Kateryna Butko, were kidnapped and held by Crimean separatists and local Berkut riot police for several days, during which they were threatened. Oles Kromplyas, a journalist and photographer with Glavkom portal, and driver Eugene Rakhno, were also taken with the women, and their abductors confiscated their laptops, memory cards, camera batteries and online video streaming equipment. They were later released to mainland Ukraine. Levko Stek, a multimedia and online journalist with Radio Free Europe/Radio Liberty, was kidnapped by unknown persons in Crimea on March 17, the day after the Crimean referendum. The assailants pulled him off a bus in the town of Bakhchisaray, handcuffed him, and pulled a bag over his head. They then drove him around in a car for a few hours before leaving him in a field with warnings not to come back to Crimea.

As the unrest after the annexation of Crimea spread to Eastern Ukraine, several online journalists also suffered attacks and pressure from pro-Russian forces there. After publishing reports critical of the separatists, Alexander Belinsky, editor of Gorlovka.ua, was kidnapped on April 14 by separatists in Gorlovka, Donetsk region, but was released shortly after negotiations. On April 12 in Donetsk proper, a car belonging to Alexei Matsuka, editor and journalist of the Novosti Donbassa portal was

---

set on fire. Additionally, on April 13, citizen journalist Artyom Deynega, who streamed live video from separatist attacks on the Security Service headquarters in Slavyansk, Donetsk region, was taken from his apartment by unknown persons. He was released on May 2, 2014.

Cyberattacks became a more common tactic in Ukraine during the Euromaidan protests, with both antigovernment and progovernment sites attacked and individual users hacked. In October 2013, Oksana Romaniuk, a prominent freedom of expression activist in Ukraine and director of the Institute for Mass Information (IMI), suffered a technical attack in which her email and computer were hacked; information stolen during the attack later appeared in disparaging articles published by a spoof online newspaper made to look like a real news outlet. The hackers also published all of her personal files on a website that seemed to be linked to the spoof newspaper.

During the protest period, hackers worked actively against government websites, with Anonymous and other groups attacking key ministry sites and other institutions in a show of indignation at the actions of Yanukovych and his government. As the crisis in Crimea unfolded, the self-proclaimed pro-Russian Ukrainian hacker group, “Cyber Berkut,” claimed to have hacked several NATO websites in protest of Western involvement in the conflict. In March 2014, the Ukrainian Security Service stated that Ukraine’s telecommunications system came under attack from equipment installed in Russian-controlled Crimea, which was used to interfere with mobile phones of members of parliament (MPs would get mass incoming calls to their numbers every 30 seconds, effectively blocking their phone). The “Cyber Berkut” also claimed to have hacked the inboxes of the regional offices of opposition parties UDAR and Batkivshchyna and posted their content online.

83 Tymur Vorona, Пророссийские хакеры «КиберБеркут» уже вторую неделю атакуют украинские сайты и телефоны политиков [Pro-Russian Hackers “Cyber Berkut” Have Been Attacking Ukrainian Websites and Politicians’ Phones for Two Weeks], AIN.ua, March 19, 2014, http://ain.ua/2014/03/19/516603.
Before and during the Euromaidan protests, there were numerous DDoS attacks on independent media websites\(^85\) and Euromaidan online communities,\(^86\) aimed at undermining their work. However, the Ukrainian internet as a whole remained largely intact and a reliable source of information on the protests, a fact which Renesys attributes to the distributed and diverse infrastructure of internet access channels in Ukraine.\(^87\)

---

85 Twitter account of KyivPost reports their website is down due to a DDoS attack, Twitter, December 9, 2013, [https://twitter.com/KyivPost/status/410081008902348800](https://twitter.com/KyivPost/status/410081008902348800).


United Arab Emirates

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>13</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>31</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>66</td>
<td>67</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

| Population:                                | 9.3 million |
| Internet Penetration 2013:                 | 88 percent  |
| Social Media/ICT Apps Blocked:             | Yes         |
| Political/Social Content Blocked:          | Yes         |
| Bloggers/ICT Users Arrested:               | Yes         |
| Press Freedom 2014 Status:                 | Not Free    |

Key Developments: May 2013 – May 2014

- The state continued to block certain political and social websites, including foreign websites that are viewed as sympathetic to the Muslim Brotherhood (see Limits on Content).

- In July 2013, Dubai police arrested a 22-year-old Indian migrant worker for uploading a video to YouTube showing an Emirati man assaulting an Indian bus driver after a car accident. If convicted, the YouTube user faces a harsher punishment than that which could be doled out to the alleged assaulter (see Violations of User Rights).

- As part of the “UAE94” trial involving prisoners of conscience, five Emiratis were sentenced to prison terms of 7 to 10 years for their online activities. In total, 69 out of the 94 political detainees were sentenced on numerous charges (see Violations of User Rights).

- A handful of bloggers and Twitter users who spoke out online against the treatment of the “UAE94” prisoners of conscience have since been arrested for their comments, with four users handed sentences of two to five years (see Violations of User Rights).

- Shezanne Cassim, an American citizen detained in April 2013 for producing a YouTube parody video on Emirati youth culture, was released in January along with others involved in the video (see Violations of User Rights).
Introduction

The government of the United Arab Emirates (UAE) has embraced information and communications technology (ICT) as a means of developing a competitive economy and improving citizen services. The internet was introduced to the country in 1995 and internet penetration has quickly risen.\(^1\) However, while remaining open 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.

More recently, dozens have been detained for their political discussions on online forums and social media. Many have indicated that they were held without charge, denied the right to an attorney, and tortured. Mobile phones must be registered and some Voice-over-Internet-Protocol (VoIP) applications are banned to facilitate government monitoring and protect the state’s monopoly on phone services. The country’s two mobile phone and internet service providers (ISPs) are either directly or indirectly owned by the state, thereby facilitating government requests for surveillance data. Numerous crackdowns on users have increased self-censorship on social media and online news outlets, the most prominent of which are government-owned.

The wealthy Gulf state has taken several moves to restrict access to online tools that challenge the government’s authoritarian grip on both politics and telecommunications. 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 social matters. Responding to the growing use of social media to call for political reforms and document government abuses, a new cybercrime law was issued in 2012. The law provides harsh punishments for a wide range of vague offenses, such as criticizing the country’s rulers and religion. These laws, combined 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.

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. However, for the most part, these efforts have not been tolerated by the authorities, who have responded with numerous arrests and lengthy jail sentences handed to internet users. In July 2013, 69 Emiratis were sentenced as a part of the unfair trial of 94 political detainees, known as the “UAE94.” Five of the detainees—Khalifa al-Nuaimi, Rashid al-Shamsi, Musabeh al-Rumaity, Abdullah ala-Hajri, and Omran al-Radhwan—were given prison sentences of 7 to 10 years for their online activities. Many others were arrested and imprisoned over the coverage period for commenting on the UAE94 trial, uploading footage of human rights violations, or producing satirical videos on YouTube. These cases demonstrate authorities’ zero tolerance for government criticism, including through comedy, in an environment where internet users continue to face many challenges to freedom of expression online.

---

Obstacles to Access

Similarly to other Gulf States, Emirati users enjoy a robust ICT infrastructure and high connection speeds. The number of internet users has risen rapidly: the ITU measured the internet penetration rate at 88 percent by the end of 2013, compared to 63 percent in 2008. As of May 2014, there were 1.08 million internet subscribers, 99.9 percent of whom had broadband connections. In the International Telecommunication Union’s (ITU) 2012 ICT Development Index, the UAE ranked 45th in the world and among the top five in the region. The ITU’s Measuring the Information Society (MIS) 2013 report ranked the UAE 33rd in the world.

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 29 in the ITU’s 2012 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. Prices have been steadily dropping in recent years and, in May 2012, the telecommunications company Etisalat announced a further 50 percent cut in broadband subscription costs. In August 2013, the telecommunications company “du” was criticized for its plans to automatically upgrade customers on the most basic package, which costs AED 199 (US$54) per month, to one costing AED 275 ($74) per month.

The UAE has one of the highest mobile phone penetration rates in the region at nearly 172 percent, or 16 million subscribers, by the end of 2013. In 2013, a report by the Telecommunications Regulatory Authority (TRA) ranked the country first in the world for smartphone penetration, with 73.8 percent of consumers owning smartphones. According to the same report, the overall mobile penetration rate in the country stands at 181 percent.
According to UNICEF, literacy in the Emirates was reported at 94 percent among males and 97 percent among females, thereby not constituting a strong obstacle to internet use. In 2006, the country decided to include computer labs in public schools, thereby seeking to improve computer literacy among the youth. In a review of its 2013 achievements, the UAE's Ministry of Education stated that all of its curricula were made available at Apple’s “App Store,” allowing students to view schoolbooks on an iPad. The ministry has also initiated the Durusi project with Etisalat and Google, turning school lessons for grades 11 and 12 into videos. With school infrastructure using state-of-the-art technology and tools, UAE schools are now among the top 25 worldwide for online connectivity. Among many things, “Mohammed bin Rashid Smart Learning Program” educational reform program equips teachers and students with tablet computers. There are now 123 smart-learning schools, compared with only 14 in 2012. The ministry has also completed the e-content project in both English and Arabic. Principals are enrolled in international computer literacy training programs.

The two ISPs in the UAE are Etisalat and “Du.” Both companies have launched their own carrier-neutral international internet exchange points, Smarthub and Datamena, respectively. 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 damage to submarine cables affected internet bandwidth. 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. Du suffered similar disruptions in April 2010 and March 2011 due to cuts to the SEA-ME-WE 4 cable. 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.

Both telecommunications companies 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, while a majority of Du is owned by various state companies. Etisalat used to dominate the telecommunication market until 2006, when Du was granted a working license. Since 2006, no new providers have been licensed, though there is no information on whether new applications were submitted. The two companies are also the major mobile phone operators.

Providers fall under the laws and regulations set by the Telecommunications Regulatory Authority (TRA), which has been headed by Mohamed Nasser Al Ghanim since its establishment in 2004. The TRA's tasks include licensing, conducting surveys, promoting investment, and assigning websites to the “.ae” top-level country domain.23

**Limits on Content**

Online censorship has increased in the UAE following the regional uprisings of 2011. The authorities have 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. Twitter, for example, is highly important in an online media landscape that is dominated by state-run news sites that refuse to cover controversial trials or stray too far from the state’s overall narrative. These factors contribute to a highly-controlled online environment in which freedom of expression and the right to information are not respected.

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. In November 2013, a report by CitizenLab found that a number of websites have been misidentified as containing nudity or pornographic content by the filtering tools SmartFilter (used by Etisalat) and NetSweeper (used by Du), resulting in their blocking in the UAE.24 Additionally, a January 2013 report found five installations of Blue Coat ProxySG—which contains a web filtering system—in the country's network, linked to Etisalat.25

Although YouTube, Facebook, Twitter, and international blog-hosting services are freely available, controversial terms are often filtered from search results within these sites. The TRA, working with the Ministry of Communications, has also blocked 500 search terms.26 For example, some parts of Flickr are still blocked in the UAE, including the “advanced search” function.27 Users reported that the search results page is blocked on YouTube when searching “Chicken Breast”28 or “Like a Virgin.”29 A number of Twitter users called on their followers to get Tumblr unblocked by filling out an online form for both providers.30

---

27 See, for example, [https://twitter.com/nraford/status/340020487033864192](https://twitter.com/nraford/status/340020487033864192).
28 See [https://twitter.com/EM_J/status/218282557833274112Without](https://twitter.com/EM_J/status/218282557833274112Without).
29 See [https://twitter.com/hghareeb/status/175634654920048640](https://twitter.com/hghareeb/status/175634654920048640).
30 See [https://twitter.com/DemetriasLooch/status/375423348261408769](https://twitter.com/DemetriasLooch/status/375423348261408769).
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.\(^{31}\) Skype’s download page and online forum continue to be blocked, alongside several proxy websites. In April 2014, Etisalat explained over Twitter that Skype can only be used over Wi-Fi.\(^{32}\) 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, a site that unblocks censored YouTube content,\(^{33}\) as well as the chatting website Omelga\(^{34}\) and the image-based social network “We Heart It.”\(^{35}\)

The website “Cairo Portal” reported being blocked in the UAE, along with other unnamed Egyptian websites, following their critical reports of the country’s support for the military leadership in Egypt.\(^{36}\) Authorities continue to ban inactive sites such as the political forum “UAE Hewar” and the blogs “Secret Dubai Diary”\(^{37}\) and “UAE Torture.”\(^{38}\) The latter posted a 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.\(^{39}\) A request to unblock UAE Hewar was rejected by the Federal Supreme Court in July 2012,\(^{40}\) and its Facebook page is also blocked due to its criticism of the regime and state corruption.\(^{41}\) As part of a verdict, in which five users were sentenced 7 to 15 years for violating the constitution and cooperating with foreign political organizations (see “Violations of User Rights”), a court also ordered the blocking of five websites that are 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 Yanabeeaa.net educational network.\(^{42}\)

The Lebanese queer and feminist e-magazine Bekhsoos\(^{43}\) and the U.S.-based Arab Lesbian e-magazine Bint El Nas are both blocked.\(^{44}\) Many websites displaying religious content are blocked, including an Arab Christian online forum named The Church Network.\(^{45}\) In the past three years,
United Arab Emirates

political content has been the focus of state censorship. Examples include the secular pan-Arab online forum “Modern Discussion”, and the California-based Arabic online newspaper *Watan*, all blocked in September 2012. A website disseminating news of the trial of 94 Emirati political detainees was also blocked in 2013. The anonymous websites “UAE University Watch” and “UAE Prison,” which exposes violations against jailed expatriates, have both been 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.

The availability of Voice-over-Internet-Protocol (VoIP) services in the UAE has been shrouded in doubt and disputes between the country’s two telecommunications companies and the TRA. In the past, many aspects of VoIP applications were blocked by ISPs, and Skype was classified by the TRA as an “unlicensed VoIP.” However, on March 19, 2013, Du subscribers suddenly reported no obstacles in accessing the Skype website or in making Skype-to-phone calls. Etisalat announced that it would follow suit one month later. After initial reports from the TRA indicated that Skype users could still face fines of AED 1 million (US$272,000) or two years imprisonment, the regulatory body denied that it had made these statements and reiterated that Skype was still an “unauthorized service.”

Before these events, a notice appeared on the Skype home page stating, “Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE’s Internet Access Management Policy.” Similar products such as Viber or Apple’s Facetime were also banned; 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 and Facetime are accessible over Wi-Fi, though only if the applications are downloaded outside of the country.

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. In January 2014, the VoIP service “Vippie by Voipswitch” tweeted that they were blocked in the Emirates. Despite these limitations, circumvention software

---

50 See [http://uaeprison.com/](http://uaeprison.com/).
51 See [http://www.emaratybedoon.blogspot.com/](http://www.emaratybedoon.blogspot.com/).
58 See [https://twitter.com/Vippie_/status/423058434947178496](https://twitter.com/Vippie_/status/423058434947178496).
and proxies are commonly used by Emiratis to access blocked content59 and VoIP services.60 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.61 On numerous occasions the TRA has emphasized that it is up to mobile phone providers to license these products. Etisalat and Du currently offer their own prepaid VoIP cards, although their prices are higher than those listed by Skype.

Intermediaries do face possible charges for content posted or appearing on their websites. Under the 2012 cybercrime law, website owners and employees “may be held liable” for any violations occurring on their sites, including defamation charges.62 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.63 In a case dating from July 2009, a court suspended the website and newspaper Al Emarat Al Youm for 20 days for running a story about the doping of a race horse owned by the president’s two sons.64

Decisions to block or remove online content often lack procedural transparency or judicial oversight. On its website, the telecommunications company Du details what criteria it uses to block websites. 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.65

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.66 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.67 Etisalat and “du” have responded to Twitter users about unblocking inquiries by asking them to fill out certain online forms, yet there is no information on whether the bans were lifted.68

68 See https://twitter.com/Etisalat_Care/status/417654518768074753 and https://twitter.com/dutweets/status/414787641620430848Evans.
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 suffering such 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. 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 fears 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. Nonetheless, users have access to a variety of local and international news outlets, even if there are disparate reports of blocking specific UAE-related articles from these sites.

Social media use has increased in recent years, in line with regional trends. Facebook recently hit 3.6 million users in the UAE, representing a penetration of 61 percent. By the end of 2013, 6.2 percent of internet users in the UAE had active Twitter accounts. While the UAE did not witness protests on a scale similar to its Arab neighbors, Emiratis created petitions calling for reforms and conducted online activism to expose corruption and demand change. Families of political prisoners still rely on Twitter to speak on behalf of detainees, explaining their cases, spreading information about violations to their rights, and calling for their release. There are several examples of relatives who are active online, including Mariam al-Mansouri, the wife of detained blogger Rashid al-Shamsi, and Aysha al-Thufiri, the daughter of detainee Salih al-Thufiri.

---


71 See https://twitter.com/ECHRIGHTS/status/230334658129321985.


74 See https://twitter.com/MariamMansori.

75 See https://twitter.com/Aysha_75.
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, publishing law, and 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 2013 and early 2014, with at least five users sentenced to prison for three to five years.

Article 30 of the country’s 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. In 2012, the president of the UAE appointed himself as head of the judiciary, overtaking the position of the minister of justice. 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. Furthermore, former detainees who have since been pardoned are continually harassed and do not enjoy their full rights as citizens.

Articles 8 and 176 of the penal code are used to punish public “insults” of the country’s top officials, although these provisions are widely used to prosecute any users who express a desire for political reform. Articles 70 and 71 of the 1980 publishing law prohibit criticism of the head of the state and of Islam or any other religion. 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).

In January 2011, the editor of Hetta.com was fined and his website was blocked for a month after a court upheld a defamation suit brought by the Abu Dhabi Media Company over defamatory and offensive user comments on the website. In July 2011, Abu Dhabi police warned that spreading
rumors through text messages constitutes libel and can be punishable by up to three years in jail. In April 2012, a spokesperson for the Ministry of Interior Affairs stated on a local TV channel that the ministry has “electronic patrols” tracking all “topics and materials written and shared on social networks.” He added, “Anything [in] violation of the law at these web sites will be considered as abuse and will be punishable as in the real world.”

A new cybercrime law was issued in November 2012, replacing an earlier decree from 2006 that was criticized for being too vague. 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.

Authorities regularly make use of these laws to prosecute Emirati citizens and residents for their online activities. In July 2013, Dubai police arrested a 22-year-old Indian migrant worker for uploading a video showing an Emirati man assaulting an Indian bus driver after a car accident. The assaulter's son submitted a complaint to the police against the person who has uploaded the video for “defamation.” Dubai Police confirmed the arrest and clarified that the uploader should have submitted the video to them instead of sharing it, which violates the privacy of the assaulter. According to Arabian Business, the man who uploaded the video now faces up to two years in jail for defamation, while the assaulter, a senior Emirati official, faces only a year in jail or a maximum fine of AED 10,000 (US$2,700) for minor assault. In November 2013, a spokesperson from the ministry of interior said people who upload photos of others without their permission could face a minimum prison sentence of six months and/or a fine of up to AED 500,000 (US$136,000). Foreigners and homosexuals also face targeting by the authorities. In June 2013, a gay man from Kenya was

reportedly entrapped by Dubai police after they contacted him through a gay-dating website. There was little information to confirm or follow-up on the arrest. Under UAE law, foreigners can be imprisoned or deported for violating the moral code.

In a case that made international headlines, Shezanne Cassim, a Sri Lankan-born American citizen living in the Emirates, was arrested in April 2013 for creating and uploading a parody video of youth culture in the UAE. The video, posted in October 2012, included a clear warning, stating, “The following events are fictional and no offence was intended to the people of Satwa and UAE.” Cassim spent five months in jail before he was formally charged with “defaming the image of UAE society abroad.” In December 2013, Cassim and two Indian men were sentenced to one year in jail and a fine of AED 10,000 (US$2,723). A Canadian woman, a British woman, and an American man were given the same sentence in absentia. Two Emirati brothers involved in producing the video were given eight months in jail and a fine of AED 5,000 (US$1,360), while a third was pardoned. In December 2013, an Emirati named Obaid al-Zaabi was arrested immediately after appearing on CNN to discuss the case of Cassim, with whom he had shared a prison cell. Al-Zaabi had been previously arrested in July 2013 for his pro-reform and human rights views on Twitter. In January 2014, Cassim and others detained with him were released. He was deported to the United States.

The key development over the past coverage period was the July 2013 sentencing of 69 political prisoners as part of a mass trial of 94 citizens, known as the “UAE94” trial. Twenty-five citizens were acquitted. Many of the detainees that make up the UAE94 are members of the Reform and Social Guidance Association, better known as al-Islah, which seeks political reform and a greater adherence to Islam in society. As mentioned, al-Islah members often engage in political debates online and seek to document and disseminate information on human rights violations on social media. These detainees were given jail sentences of 7-15 years for being part of an organization with intent to overthrow the government and with ties to Egypt’s Muslim Brotherhood. Reacting to Egypt’s 2011 parliamentary elections, in which the Muslim Brotherhood’s Freedom and Justice Party gained more seats than any other political party, Dubai’s chief of police tweeted that “since Muslim Brotherhood has ‘become a state,’ anyone advocating its cause [in the UAE] is considered a foreign agent.”

Among those sentenced in July 2013 were blogger Khalifa Al-Nuaimi\textsuperscript{102} and Twitter users Rashid al-Shamsi\textsuperscript{103} and Musabeh al-Rumaithy,\textsuperscript{104} three individuals arrested for their online activities and sentenced to 10 years imprisonment.\textsuperscript{105} Blogger Abdullah al-Hajri\textsuperscript{106} and Twitter user Omran al-Radhwan\textsuperscript{107} were also sentenced to seven years.\textsuperscript{108}

The authorities also target social media users for posting content that exposes human rights abuses or criticizes government practices, particularly their handling of cases related to political detainees and prisoners of conscience such as those in the UAE94 trial. Two family members of UAE94 prisoners were arrested in July 2013, immediately after their sentencing, for social media posts calling for Emiratis to break the silence surrounding the mass trial and to call for political reform.\textsuperscript{109}

In September, al-Islah member Khalid Suweidi was reportedly detained after tweeting his support for members of the UAE94 trial.\textsuperscript{110}

Osama al-Najjar was arrested in March 2014 for Twitter posts in which he expressed support for his imprisoned father, Husain al-Najjar, a member of the UAE94.\textsuperscript{111} Security forces, lacking a warrant, raided his house and confiscated his electronic devices. In the last tweet before his arrest, he defended his father in a rhetorical response to a radio address from the ruler of Sharjah.\textsuperscript{112} His first hearing was not held until September 2014, when he was able to meet with a lawyer for the first time since his arrest. He faces charges of “designing and running a website on social networks with the aim of publishing inaccurate, satirical and defamatory ideas and information that are harmful to the structure of State institutions,” as well as with “contacting foreign organizations” to spread false information and belonging to al-Islah.\textsuperscript{113}

These arrests are particularly problematic given the high number of long prison sentences that have been doled out for similar online activities. Twitter user Waleed al-Shehhi was sentenced to two years imprisonment and handed a fine of AED 500,000 (US$136,000) in November 2013 under

\textsuperscript{102} Al-Nuaimi had previously written about “the UAE 5” and had been consistently threatened prior to his arrest. See https://kalnuaimi.wordpress.com/.
\textsuperscript{103} Al-Shamsi had tweeted news of arrests and written blog posts related to politics and free speech See http://rashedalshamsi.blogspot.fr/.
\textsuperscript{104} 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 “Another Emirati activist banned from Travel,” Watan, June 28, 2012. http://bit.ly/19bVlBW.
\textsuperscript{106} Al-Hajri was arrested over the contents of his blog, http://alhajria.wordpress.com, in which he called for more government action to combat public immorality.
\textsuperscript{107} 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.
\textsuperscript{112} See https://twitter.com/O.Hussain_/status/445271293764833280.
United Arab Emirates

Articles 28 and 29 of the cybercrime law, which provide punishments for “endangering state security” and “harming the reputation of the state.” He was arrested in May 2013 for his open support of political detainees.

In March 2014, 35-year-old businessman Khalifa Rabeiah and 40-year-old Etisalat engineer Othman al-Shehhi were sentenced to five years in jail and given a fine of AED 500,000 (US$136,000). The two were convicted of violating Articles 24 and 41 of the cybercrime law, which criminalize the use of the internet to “damage national unity or social peace.” Rabeiah and al-Shehhi, both members of al-Islah, had been arrested in July 2013 for Twitter posts that were critical of judiciary procedures relating to political detainees. The two men were reportedly detained in an unknown location for six months, tortured, and denied the right to legal aid.

In December 2013, 19-year-old blogger Mohammed Salem al-Zumer was sentenced to three years in jail and given a fine of AED 500,000 (US$136,000) for “insulting the country’s leaders” and “defaming the security apparatus” through his Twitter and YouTube accounts. He had been arrested in December 2012 after accusing Emirati authorities of torturing detainees (such as his uncle, Khaled al-Nuaimi) and of hiring Blackwater, a private security company, to harass protesters. According to his mother, the blogger has been held in solitary confinement, tortured, and pressured into making a confession stating that Khalifa al-Nuaimi, another UAE94 defendant, had encouraged him to edit and upload the videos.

Abdulrahman Omar Bajubair was sentenced to five years in absentia in December 2013 for defaming the judiciary over his coverage of the UAE94 trial. He is currently based in Qatar. The Arabic Network for Human Rights Information (ANHRI) and the Gulf Center for Human Rights reported he was targeted for running the blog-campaign Motadaminoon in solidarity with prisoners, while the Emirates Centre for Human Rights added that he was specifically targeted for what he was posting.

---

116 Twitter profile [https://twitter.com/binrabeiah](https://twitter.com/binrabeiah).
117 Twitter profile [https://twitter.com/OthmanAlShehhi](https://twitter.com/OthmanAlShehhi).
120 BBC. “UAE authorities ‘detain 18-year-old blogger.’” 7 December 2012, [http://bbc.in/VPHeyP](http://bbc.in/VPHeyP).
122 ANHRI. “Two Emirati online activists sentenced to jail under recent cybercrimes law,” Iflex, January 3, 2014, [http://www.ifex.org/united-arab_emirates/2014/01/03/online_activists_jailed](http://www.ifex.org/united-arab_emirates/2014/01/03/online_activists_jailed/).
through the blog’s Twitter account as well as the account “@intihakat,” which reports on violations against political detainees.\(^{127}\)

Arrested in March, Abdulhamid al-Hadidi was sentenced in April to ten months in jail under Article 46 of the cybercrime law and Article 265 of the penal code for allegedly “spreading false information” about the trial of the so-called UAE94, of which his father, Abdulrahman al-Hadidi, is a member.\(^{128}\) Al-Hadidi had been active on social media by sharing news from detainees and details of their trials. He was also pushing detainees’ families to work together to demand fair and transparent trials for the accused, as well as an end to state violations against their rights to prison visits. Al-Hadidi was released from prison in November 2013.\(^{129}\)

In addition to arbitrary detentions, unfair prosecutions, and torture, online activists also face a range of extralegal attacks in the UAE. In October 2012, blogger Ahmed Mansour faced media harassment and physical beatings. The actions were taken in response to a pre-recorded speech he made that was later broadcast at a side event to the United Nations Human Rights Council regarding violations in the UAE, Oman, and Saudi Arabia.\(^{130}\)

The high amount of prosecutions and physical harassment of users in the UAE is, in part, due to the several obstacles they face in using ICT tools anonymously. In January 2013, the country’s two mobile phone providers gave a last warning to their users to register their SIM cards or have their service discontinued for failing to comply.\(^{131}\) The government had required every mobile user to re-register their information as part of the TRA’s “My Number, My Identity”\(^{132}\) campaign launched in June 2012.\(^{133}\) Cybercafe customers are also required to provide their ID and personal information in order to surf the net.\(^{134}\)

Internet and mobile providers are not transparent in discussing the procedures taken by authorities to access their data and users’ information. Warnings from both the Abu Dhabi and Dubai police against spreading rumors through mobile messages may indicate the government’s overall surveillance of ICT users.\(^{135}\) Further, Twitter users have been arrested for exchanging private

\(^{127}\) ECHR. “19-year-old Emirati activist jailed for tweets.” December 25, 2013. \url{http://www.echr.org.uk/?p=1104}


\(^{129}\) “Emirati jailed for twitter comments is freed as others face prison,” Emirates Centre for Human Rights, November 3, 2013, \url{http://www.echr.org.uk/?p=1001}.


\(^{132}\) 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. \url{http://www.tra.gov.ae/mynumber.php}.


messages with a controversial account. Saeed al-Shamsi was detained on December 14, 2012 over suspicions that he ran the anonymous Twitter account “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. 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 later, five more Twitter users were arrested for expressing political criticism and support for detainees. No reports followed their arrests or disclosed further details on their cases.

Incidents of providers demanding warrants or legal permission for security bodies to gain access to user data are not known. In 2009, the makers of BlackBerry devices alleged that a software update issued by the UAE telecommunications company Etisalat was actually spyware used to “enable unauthorized access to private or confidential information stored on the user’s smartphone.”

The UAE remains one of the top countries facing hacking attempts worldwide. In September 2013, Abu Dhabi Police warned businesses “of a surge in attacks by international hackers” and advised them to use necessary software for protection and to restrain from using personal emails for work communication. The TRA has also announced new measures to block spam emails and SMS. Six hackers were arrested last year in New York after stealing debit card data from the National Bank of Ras Al-Khaimah in the United Arab Emirates and Bank Muscat in Oman in two attacks in December 2012 and February 2013, according to U.S prosecutors. Experts estimate that three-quarters of internet users in the UAE will become victims of cybercrime. Seventy-five percent of the hacking is expected to target bank accounts. In late 2012, a report recorded the country’s spam rate 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. In July 2012, the TRA denied claims that the hacktivist group Anonymous “penetrated the country’s proxy server and extracted a list of blocked website addresses.”

---

United Arab Emirates

Emirati activists have also reported spyware and malware attacks against their computers. In one case from January 2013, a user received an email 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.146

United Kingdom

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internet Freedom Status</strong></td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td><strong>Obstacles to Access (0-25)</strong></td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>Limits on Content (0-35)</strong></td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td><strong>Violations of User Rights (0-40)</strong></td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td><em><em>TOTAL</em> (0-100)</em>*</td>
<td>23</td>
<td>24</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 64.1 million

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Penetration 2013:</td>
<td>90 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 2014 Status:</td>
<td>Free</td>
</tr>
</tbody>
</table>

Key Developments: May 2013 – May 2014

- Filtering mechanisms, particularly child-protection filters enabled on all household and mobile connections by default, inadvertently blocked legitimate online content (see Limits on Content).

- The Defamation Act, which came into effect on 1 January 2014, introduced greater legal protections for intermediaries and reduced the scope for “libel tourism,” while proposed amendments to the Contempt of Court Act may introduce similar protections for intermediaries in relation to contempt of court (see Limits on Content and Violations of User Rights).

- New guidelines published by the Director of Public Prosecutions in June 2013 sought to limit offenses for which social media users may face criminal charges. Users faced civil penalties for libel cases, while at least two individuals were imprisoned for violent threats made on Facebook and Twitter (see Violations of User Rights).

- In April 2014, the European Court of Justice determined that EU rules on the mass retention of user data by ISPs violated fundamental privacy and data protection rights. UK privacy groups criticized parliament for rushing through “emergency” legislation to maintain the practice in July, while failing to hold a public debate on the wider issue of surveillance (see Violations of User Rights).

- Police asked a Twitter user to delete a non-threatening tweet about the UK Independence Party (UKIP); separately, intelligence agents raided the offices of the Guardian and ordered the destruction of hard drives after the newspaper published leaked documents about government surveillance (see Violations of User Rights).
Introduction

The United Kingdom (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 result of the growing popularity of smartphones and the increasing availability of superfast networks, which have maximum advertised speeds of 30 Mbit/s or more. But a growth in technological capacities has simultaneously allowed expanded surveillance, leading to growing fears of abuse by police and intelligence agents.

Leaks by former National Security Agency (NSA) contractor Edward Snowden, published in the Guardian, revealed the extent of digital surveillance by the Government Communications Headquarters (GCHQ), a British intelligence-gathering agency. Leaked documents outlined programs and tactics used by GCHQ and its international partners over the past several years, raising questions about the reliability of any previous measures of users’ online freedoms in the UK. The fact that these tactics were apparently lawful led to concerns about proportionality, and whether existing legislation on surveillance was intended to be applied in digital contexts.

As in past years, the increasing use of technological methods to restrict access to certain content continued to be controversial. The outsourcing and privatizing of blocking and filtering services raised questions about transparency and overblocking, which may have significant effects on users’ online freedoms. There have also been indications that internet users may not fully comprehend their rights and responsibilities in the online world, leading to more prosecutions for online activity.

On a more positive note, changes to the Defamation Act, which came into effect on 1 January 2014, have resulted in more protections for intermediaries and defendants. Proposals for revisions to the Contempt of Court Act were also introduced to deal with the effects of online reporting of the administration of justice. Attempts to curtail online copyright infringements in the form of the Digital Economy Act, which had been criticized for their possible impact on net freedoms, have stalled. While some legislation is therefore being updated and promulgated to protect online freedom, the UK’s legislative landscape may need to be revisited to safeguard users’ online freedoms in the era of mass surveillance.

Obstacles to Access

Access to the internet has become essential to citizenship and social inclusion in the UK. ICT infrastructure in the country is generally of a strong standard, allowing high levels of access. Over the past year, substantial investments in superfast broadband have also 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. Policies and regulation in the country tend to favor access, although recent revelations regarding extensive government surveillance practices may impact how citizens choose to access the internet.

---

Internet penetration has grown from 78.39 percent in 2008 to 89.84 percent at the end of 2013, with more than 80 percent of adults having household internet access. In the past year, the share of homes with fixed and mobile broadband has grown to 77 percent, with 26.7 percent of UK households having superfast broadband. Nearly 100 percent of all households are within range of ADSL connections and 48 percent of households are within reach of cable. In June 2013 the government completed a consultation that reinforced the need for a supportive policy and regulatory environment for investment in broadband infrastructure, and pledged a further GBP 530 million (US$ 850 million) to help make superfast broadband available in rural communities. The government also set a target that 95 percent of the population would have access to superfast broadband by 2017, and by March 2014, 509,000 rural premises had such access. This builds on the previous phase in which the Broadband Delivery UK program made GBP 830 million (US$ 1.32 billion) available for broadband expansion. The extension of fast broadband to all areas remains a priority and steady progress to this end continues.

Mobile telephone penetration is extensive, with a reported penetration rate of 123.7 percent at the end of 2013. In 2014, 61 percent of all UK adults claimed to own a smartphone, leading to a substantial growth of internet use on mobile phones. 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 6 million subscriptions and over 70 percent of UK premises being able to access outdoor 4G coverage from at least one network. Second-generation (2G) and third-generation (3G) networks are available in over 99 percent of all households. Only four percent of households use mobile broadband as their main internet connection, and overall household use of mobile broadband has decreased over the past two years, from 17 percent in 2011 to 8 percent in March 2014.

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 socio-economic 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 by 11 percentage points since 2008. Of the UK households that do not have access to the internet, the majority have no intention to get connected.

The average broadband speed in 2014 was 17.8 Mbps, continuing a trend of rising speeds and growing satisfaction among consumers served by faster fiber-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 57 percent of adults said they used data services on their mobile phones, an eight percent increase from 2013. More than a quarter of all fixed broadband connections are superfast, an increase of 58 percent from 2013. 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 result of a growth in broadband take-up and switching to 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 for superfast broadband has declined by eight percent to just over GBP 8 (US$ 13) per month, while fixed broadband prices increased by one percent in real terms to GBP 16.35 (US$ 26) a month in 2012. The price of a basket of mobile services fell by 3.5 percent in 2013, and is around GBP 14.30 (US$ 23.10). The difference between superfast and standard services is between GBP 5 (US$ 8) and GBP 10 (US$ 16) per month.

Four major ISPs, British Telecom (BT), Virgin Media, TalkTalk, and Sky, control 87 percent of the total market. 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 access. By 2013, unbundled telephone lines reached 9 million homes. Virgin has the highest share of superfast broadband subscribers (56 percent); BT has a 35 percent share, but is dominant in the provision of wholesale access.

United Kingdom

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 an alternative dispute-resolution scheme.\footnote{Ofcom, \textit{Consolidated Version of General Conditions of Entitlement} (London: Ofcom), December 16, 2013, \url{http://stakeholders.ofcom.org.uk/binaries/telecoms/qa/GENERAL_CONDITIONS_AS_AT_26_DECEMBER_2013.pdf}.} The government also 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,\footnote{Such as peer-to-peer (P2P) file sharing and television streaming.} while mobile providers have cut back on previously unlimited access packages for smartphones, reportedly because of concerns about network congestion. 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.\footnote{Ofcom, “Ofcom’s approach to net neutrality,” November 11, 2011, \url{http://stakeholders.ofcom.org.uk/consultations/net-neutrality/statement/}.} It described the blocking of services and sites by ISPs as “highly undesirable” but said that market forces will address potential problems.\footnote{Developments at European Union (EU) level may, in the future, also have an impact on net neutrality provisions in the UK. See \url{http://ec.europa.eu/digital-agenda/en/eu-actions}.}

In July 2012, major ISPs published a “Voluntary Code of Practice in Support of the Open Internet”.\footnote{Broadband Stakeholder Group, “ISPs launch Open Internet Code of Practice,” July 25, 2012, \url{http://www.broadbanduk.org/2012/07/25/isps-launch-open-internet-code-of-practice/}.} 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.\footnote{Broadband Stakeholder Group, “ISPs launch Open Internet Code of Practice,” May 2013, \url{http://www.broadbanduk.org/wp-content/uploads/2013/06/BSG-Open-Internet-Code-of-Practice-amended-May-2013.pdf}.}

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 be restricting offensive or otherwise inappropriate words or expressions in domain name registrations.\footnote{Nominet is the domain registrar in the United Kingdom, and manages access to newly introduced .uk, .wales, and .cymru domains.} The Nominet Board agreed to make all of the recommended changes.\footnote{Lord Macdonald QC, \textit{Review of .uk Registration Policy}, December 2013, \url{http://www.nominet.org.uk/sites/default/files/Lord%20Macdonald%20Report%20Final.pdf}.} The amended policy specifically aims to address limits on content in respect of serious sexual offences.\footnote{Lord Macdonald QC, \textit{Review of .uk Registration Policy}, December 2013, \url{http://www.nominet.org.uk/sites/default/files/Lord%20Macdonald%20Report%20Final.pdf}.}

**Limits on Content**

While there is no general law authorizing internet censorship in the UK, filtering mechanisms do operate with the aim of blocking criminal content such as child sexual abuse, sites that promote extremism and terrorism, and copyright-infringing materials. Filtering tools have also expanded to strengthen parental controls over the viewing of adult-oriented sites by children. These child
protection measures have been particularly controversial in the realm of mobile devices, where filtering criteria have often resulted in overblocking. A lack of transparency regarding sites blocked through court orders, as well as the increasing outsourcing and privatizing of filtering services, have also raised concerns.

The Internet Watch Foundation (IWF), a registered UK charity, aims to prevent access to child sexual abuse and criminally obscene adult content. The IWF compiles a blacklist of URLs containing images of child sexual abuse using a citizen’s hotline and investigations by IWF analysts, in accordance with the Sexual Offences Definitive Guideline published by the Sentencing Council under the Ministry of Justice. In cases where such content is hosted within the UK, therefore constituting a criminal offense, the IWF coordinates with the police and local hosting companies in order to have it removed. A similar system is in place for websites that depict child sexual abuse through non-photographic means, such as computer-generated images, as well as for websites containing criminally obscene adult content.

For child sexual abuse content that is hosted overseas and outside the jurisdiction of British courts, the IWF contacts international hotlines and foreign police authorities in order to have the content eventually removed from servers in the host country. However, in order to prevent British users from accessing the content in the meantime, British ISPs block access to the websites listed in the IWF blacklist using the CleanFeed filtering system, developed by the IWF and BT. Non-photographic child sexual abuse images and criminally obscene adult images do not fall under the remit of the IWF when hosted abroad.

Similar processes for the investigation of online materials inciting hatred were transferred from the IWF to TrueVision, a site that is managed by the police, in 2011.

In November 2013, Prime Minister David Cameron welcomed the introduction of new algorithmic filters by Google and Microsoft that prevent searches for child abuse imagery, and warned that if such measures were unsuccessful, legislative intervention could follow. As many as 100,000 search terms for illegal material are programmed to return no results. Laws such as the Protection of Children Act are used to prosecute individuals suspected of accessing or circulating content relating to child abuse. According to some reports, the task of creating certain filters has been outsourced to foreign companies, raising concerns about evading transparency and reporting requirements.

---

37 The IWF is a British charity funded by ISPs and the EU.
38 The Internet Watch Foundation (IWF) site is located at http://www.iwf.org.uk/.
under the Freedom of Information Act, particularly regarding how these filters work and why certain sites may be blocked without a court order.\textsuperscript{46}

The government has increased its efforts to limit access to materials defined as “extremist” on the internet.\textsuperscript{47} The Terrorism Act allows for the removal of terrorist material hosted online in the UK if it “glorifies or praises” terrorism, if it is information that could be useful to conducting terrorism, or if it urges people to commit or support terrorism.\textsuperscript{48} A Counter Terrorism Internet Referral Unit (CTIRU) was set up in 2010 to investigate internet materials, and the unit reported that it had removed more than 29,000 locally-hosted ‘pieces’ that breach UK terrorism legislation by April 2014.\textsuperscript{49} The government claims to have taken down some 15,000 instances of “jihadist propaganda” since December 2013 in the continuing fight to deny religious extremists in Iraq and Syria with tools to recruit British citizens.\textsuperscript{50} The government released a revised “Prevent Anti-Terrorism Strategy” in 2011, which also calls for limiting access to “extremist” materials in schools and public libraries and increasing efforts to remove “harmful content” from the internet.\textsuperscript{51} 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\textsuperscript{52}.

In addition to child sexual abuse, sites that incite hatred (or “hate sites”), and extremist sites, the government has also taken a proactive approach to restricting sites that have been found in violation of copyright protections. The UK High Court has continued to block sites based on copyright infringement,\textsuperscript{53} although it recently held that merely publishing a link to copyright infringing material, rather than hosting the material online, does not amount to a copyright infringement.\textsuperscript{54} This approach has since been confirmed by the Court of Justice of the European Union.\textsuperscript{55} There have been a number of cases in which courts have ordered sites, such as Newzbin


\textsuperscript{52} Home Office, CONTEST: The United Kingdom’s Strategy for Countering Terrorism: Annual Report.


and the Pirate Bay, to be blocked for copyright infringement, and to have their domain names seized based on the Copyright, Designs, and Patents Act, and other legislation. The CleanFeed system has been adapted to enable ISPs to enforce the blocks, and the list of blocked URLs is growing. The Digital Economy Act (DEA) also stipulates that sites found to have “substantial” violations of copyright can be blocked by a court order. However, an Ofcom review determined that such copyright-related blocking provisions, contained in Sections 17 and 18 of the DEA, are unlikely to be effective and should rather be used in conjunction with other measures. Under these Sections, the Secretary of State for Culture, Media and Sport is able to create regulations to allow “blocking injunctions” by the courts in order to force ISPs to block access to pirated copyright content. Despite the ostensible transparency of the legal system, obtaining copies of the copyright injunctions has proved challenging. The non-profit Open Rights Group (ORG) has consequently called for more transparency about what sites are blocked by court injunctions.

Under the EU 2002 E-Commerce Directive, hosts can be held liable if they are found to have had knowledge of illicit material, including libelous content, but have failed to remove it. This has caused hosting companies to promptly take down material when asked, with little inquiry as to the legitimacy of the demand. 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. (See “Violation of User Rights”)

The blocking policy is instituted in line with a voluntary code of practice adopted by the Internet Services Providers’ Association. While British ISPs are not required by law to implement the IWF

56 Cf. EMI Records (Ireland) Ltd and others v UPC Communications Ireland Ltd and others [2013] IEHC 274 (June 12, 2013); Dramatico Entertainment Ltd and others v. British Sky Broadcasting Ltd and others [2012] EWHC 1152 (Ch) (May 2, 2012); Twentieth Century Fox Film Corporation and others v. British Telecommunications plc [2011] EWHC 2714 (Ch) (October 26, 2011).
blocking list, the Home Office adopted rules in 2010 that prohibit government bodies from procuring services from ISPs that fail to use the list. Consumer awareness of CleanFeed is low, and the list of blocked sites remains secret in order to deter access to unlawful materials. In January 2014, a human rights audit of the IWF recommended the introduction of an independent judicial review of IWF’s operations.

Public debate about the imposition of measures that would more effectively prevent children from accessing adult-oriented material on the internet increased in the past year. In November 2013, Sky, TalkTalk, BT, and Virgin pledged to form a new joint venture to lead an awareness campaign around child safety with a marketing expenditure in excess of GBP 25 million (US$ 40 million). The group launched the InternetMatters.org portal in May 2014 to provide parents with advice for making decisions around children’s online safety. Media regulators also launched the ParentPort site in October 2011 to receive complaints about materials “unsuitable for children” across all forms of media and to provide a resource for parents for tips on parental controls.

With the rapid rise of mobile internet access, mobile filtering has also become increasingly prevalent. Due to concerns over the unsupervised use of data-enabled mobile phones by children under the age of 18, mobile internet subscriptions are sold to customers with child filters enabled by default and, depending on the provider, require either the disabling of the filters or a deliberate “opt-in” to adult content. Customers can verify their age and remove the filters by contacting their provider with proof of age. Blocked content includes pornography, hate sites, and in some cases, web forums that could potentially allow minors to interact with older users. The practice is conducted in accordance with a 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 Independent Mobile Classification Body (IMCB), originally appointed by the MBG to establish the criteria for which sites are deemed to be unsuitable for children under the age of 18, was replaced by the British Board of Film Classification (BBFC) to categorize content and calibrate internet filters. However, the process has been criticized for being subjective, insufficiently transparent, and generally problematic.

---

71 The Parentport site is located at: http://www.parentport.org.uk/.
The efficacy of such child-protection filtering measures for both mobiles and household access has been questioned. They are easy to circumvent, and can affect legitimate content. On several occasions due to technical difficulties at the ISP level, blocking decisions designed to prevent access to harmful content temporarily disabled users from accessing popular sites such as Wikipedia. The ORG has created the site “Blocked.org.uk” to allow users to report overblocking of content that poses little or no threat to child welfare, including sites on sexual education, drug awareness, and pages run by civil society and political parties. A report by the ORG and the London School of Economics (LSE), published in 2012, found that sites as diverse as Tor, eHow, and that of the British National Party, an extreme right-wing political organization, had been temporarily blocked. The latter was classified as a “hate site” by O2, apparently the only provider that operates a “URL checker” page that allows users to ascertain how a particular site has been classified. The owners and operators of sites are not notified that their sites have been blocked, with the ORG reporting 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.

Barriers to entry in news markets remain theoretically very low, recent years have seen a consolidation of online news providers, with large companies garnering more control over online news markets. Evidence submitted to a judicial inquiry on press practices led by Lord Justice Leveson in 2011 and 2012 revealed close links between these news providers and government actors. As a result of findings published in the Leveson Report in 2012, the larger media houses established the Independent Press Standards Organization, the first regulator for publishers in the country, while another initiative, the Impress Project, also aims to cater for smaller and online publishers on a voluntary basis. Publishers may receive greater protection from punitive damages through joining a regulator. The Crime and Courts Act establishes a higher risk of costs and fines for all newsgatherers, including bloggers, if they refuse to self-regulate. Publishers that decline to join, including news blogs, remain exposed to punitive damages if the publication features multiple authors and is subject to editorial control. There are, however, exceptions to costs and punitive damages exposure for certain types of publishers, including broadcasters, personal blogs, and special interest publications.

---

81 ORG, “Ten recommendations to ISPs for dealing with over-blocking,” (December 19, 2013); https://www.openrightsgroup.org/blog/2013/ukccis-overblocking.
Leveson also recommended that the Information Commissioner’s Office (ICO), an independent body that reports to parliament, should publish guidelines as to how the press should be allowed to process personal data in terms of the Data Protection Act, including data obtained, stored and transferred online. In a draft guidance published in January 2014, the ICO recognized that the definition of “journalism” should be interpreted broadly to include citizen bloggers. Thus citizen journalists making use of the internet may potentially avail themselves of the journalism defense in this legislation to avoid being held liable for misconduct related to data processing.

Users in the UK continue to enjoy wide access to free or low-cost blogging services, allowing them to express their views on the internet. YouTube, Facebook, Twitter and other international blog-hosting services are freely available but subject to the filters mentioned above. Users and nongovernmental organizations also employ various forms of online communication to organize political activities, protests, and campaigns. Civil society organizations maintain a significant presence online and have used internet platforms to promote various causes. For example, organizations such as Avaaz, Change.org, and 38 Degrees have millions of members who use social media to campaign successfully on issues. The Libel Reform Campaign, a joint project by the Index on Censorship, English PEN, and Sense About Science, successfully campaigned for changes in the libel laws that were introduced in 2014.

Violations of User Rights

While the UK has no written constitution or bill of rights, the European Convention on Human Rights (ECHR) has been incorporated into UK law through the Human Rights Act, and British courts have recognized the importance of freedom of expression and other human rights. Some positive steps have been taken with the aim of protecting user rights. Changes to the Defamation Act have resulted in more protections for intermediaries and defendants. However, extensive surveillance measures employed by government agencies cast a shadow over the strength and efficacy of protections of user rights in the UK. In addition, this year saw many indications that users may still lack an understanding of their legal obligations when publishing material online, particularly on social media. This is potentially worrying as citizens may be prosecuted for offenses related to copyright, libel, hate speech, incitement to violence, and contempt of court.

88 See http://www.avaaz.org/.
89 See http://www.change.org/.
93 See Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), accessible: http://services.parliament.uk/bills/2012-13/defamation.html.
ISPs and users may be punished for copyright-related offenses under the Digital Economy Act (DEA) of 2010. Among other things, the DEA grants the government the power to impose rules on ISPs, such as monitoring and notifying their users after they receive information or reports containing evidence of infringement, even if these allegations are not proven in a court or independent hearing. On September 11, 2013, Ofcom published research showing that almost a quarter of downloads in the UK infringe copyright. A report published in the same month by the LSE Media Policy Project challenged the notion that creative industries are suffering revenue decline as result of copyright infringements. In light of the possible social, cultural, and political impact of punitive measures against citizens, as well as the risk that incentives for innovation and growth will be weakened, the LSE report stressed the need to re-evaluate the DEA.

Over the past year, some users have been prosecuted for copyright-related offenses, with the Federation Against Copyright Theft (FACT) reporting the arrest and fining of various individuals. In March 2014, FACT also launched an Infringing Website List (IWL) in conjunction with the City of London Police to prevent illegal websites operating globally from benefitting from advertising. The IWL retains a list of copyright infringing sites for advertisers to refrain from placing advertisements on such pages. Furthermore, Sections 17 and 18 of the DEA allow for the possibility of the government authorizing “technical measures” against users, such as limiting access speeds or cutting off access altogether, in the fight against piracy. However, following an Ofcom review, the government acknowledged that it would be impracticable to enforce these Sections. In fact, a Draft Deregulation Bill was published in July 2013 that contained a provision to repeal Sections 17 and 18 of the DEA. The provision remained in a revised draft introduced in January 2014. The bill is yet to be finalized.

In June 2012, Ofcom published an Obligations Code that specifies when and how ISPs may issue warning notices to their customers who are thought to be illegally accessing copyright-infringing

---

94 Accessible: http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1
material. The code provides for a graduated (or “three strikes”) response, whereby ISPs must monitor IP addresses and send notifications to infringing users. After a user receives three notifications in a year, copyright owners may request users’ personal details and initiate legal action against them. Only ISPs providing services to over 400,000 broadband-enabled lines are required to implement the graduated response scheme, therefore exempting libraries and providers of wireless hotspots. Additionally, the “technical measures” phase of the DEA cannot be initiated until the Obligations Code is in force for 12 months. The code and relevant costs must be approved by both houses of parliament. Delays in the implementation of the code have made it unlikely that ISPs will be required to take these measures earlier than late 2015.

In June 2013, the Director of Public Prosecutions published final guidelines for prosecuting cases involving communications sent via social media. The guidelines include robust prosecution of communications that may be perceived as credible threats, specifically target an individual or individuals, or amount to a breach of a court order. By contrast, communications that are offensive, indecent, obscene, or false, are unlikely to be subject to prosecution.

The guidelines have been applied in at least one incident to protect victims of abuse or trolling on social media platforms. In late 2013, campaigners for the retention of a female figure's image on UK banknotes became the subjects of extensive harassment online. Some of the abusers were identified, and in February 2014 a man was charged under section 127 of the Communications Act for his involvement via Twitter, and later sentenced to 18 weeks in jail. In the same month, a UK citizen who set up fake Facebook accounts to ‘troll herself’ and falsely accuse family members of online abuse was sent to prison for 20 months.

In December 2013, proposed changes to the Contempt of Court Act were published by the UK Law Commission. The changes addressed the challenges new media may pose to existing laws on contempt of court, which pre-date the popular internet, among other concerns. The

---


105 Ofcom, “Online Infringement of Copyright and the Digital Economy Act 2010.”

106 The Digital Economy Act 2010 (c. 24), section 10(2).


first of its reports, which focused on juror misconduct and internet publications, made various recommendations for reform, including a defense that would prevent online publishers from having to continuously monitor all of their archived material.\(^\text{115}\) It has also been proposed that online publications by new media users fall within the ambit of traditional publication for the purposes of the act—meaning that individuals who tweet, blog, or post content that potentially prejudices the administration of justice could be held liable for contempt of court. Jurors who use the internet to look up information about a case may also face criminal charges, in accordance with the proposals.\(^\text{116}\)

Social media users have been investigated or charged for interfering with the administration of justice. In late 2013, detectives said they were investigating celebrity Peaches Geldof, who released the name of two mothers who had allegedly allowed singer Ian Watkins to abuse their babies, although their identities were protected under the Sexual Offenses Act.\(^\text{117}\) She later apologized and deleted the tweets.\(^\text{118}\) Geldof died in 2014. Legal proceedings were launched in February 2013 against several online users for publishing photos that purportedly depicted Jon Venables. A “contra mundum” court injunction bans the publication of anything that could reveal the new identities, appearances, whereabouts or movements of Venables and Robert Thompson, who as children were convicted of murdering a two-year-old.\(^\text{119}\) One received a 14-month suspended sentence and a fine of GBP 3,000 (US$ 4,850) in November 2013 for publishing a photograph on Twitter.\(^\text{120}\)

In recent years, threats of libel suits had a significant chilling effect on both content producers and ISPs, particularly due to the substantial financial and evidentiary burden on defendants.\(^\text{121}\) This was compounded by an increase in so-called “libel tourism,” a practice in which foreign litigants with little or no connection to a specific country use the ubiquity of online content to invoke plaintiff-friendly English libel laws against publishers.\(^\text{122}\) Amendments to the Defamation Act, which came into effect on 1 January 2014,\(^\text{123}\) have now placed restrictions on libel tourism by requiring claimants to prove that of all the places in which a statement was published, England and Wales is clearly the

---


123 See Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), accessible: [http://services.parliament.uk/bills/2012-13/defamation.html](http://services.parliament.uk/bills/2012-13/defamation.html).
most appropriate place in which to institute an action.\textsuperscript{124} The act also introduces a serious harm threshold which should help protect freedom of expression, and it codifies defenses of truth, honest opinion, and publications on matters that are in the public interest.\textsuperscript{125}

Nonetheless, the use of libel prosecutions for offending Twitter posts, a practice dubbed “twibel,” has increased. Some cases have resulted in substantial damages.\textsuperscript{126} In May 2013, the High Court ruled that Member of Parliament Sally Bercow had wrongfully implicated politician and businessman Lord Alistair McAlpine in a child abuse scandal via a libelous tweet.\textsuperscript{127} Bercow apologized, removed the offending material, and settled out of court with McAlpine for GBP 15,000 (US$ 24,000).\textsuperscript{128} However, the libelous tweet was also retweeted by some of Bercow’s thousands of followers. McAlpine settled out of court with at least one of these followers, comedian Alan Davies,\textsuperscript{129} while he also demanded that others who had retweeted Bercow’s tweet should donate funds to a charity of his choice.\textsuperscript{130} McAlpine died in 2014.

The government has also taken measures against users who publish or download information perceived as a security threat. General laws such as the Public Order Act and the Communications Act are being used to charge individuals with crimes for posting threatening or harassing materials on the internet.\textsuperscript{131} In the so-called Twitter joke case in 2010, for example, Paul Chambers was convicted under Section 127 of the Communications Act for jokingly tweeting that he would “blow up” a local airport. The High Court overruled his conviction in July 2012, finding that the tweet was not of menacing character.\textsuperscript{132}

There are no public restrictions on the use of encryption technologies. However, under Part 3 of the 2000 Regulation of Investigatory Powers Act (RIPA), it is a crime not to disclose an encryption key upon an order from a senior policeman or a High Court judge.\textsuperscript{133} The Court of Appeal held in 2008 that such disclosure would not necessarily violate the privilege against self-incrimination.\textsuperscript{134} The provision has been used to obtain court orders to force disclosure of keys. Between April 1, 2013

\begin{thebibliography}{99}
\bibitem{Defamation Act 2013} Defamation Act 2013 (c. 26); see John Aglionby, “UK Defamation Act aims to end trivial claims and libel tourism,” Ft.com, December 31, 2013, http://www.ft.com/cms/s/0/afe77e0c-7204-11e3-bff7-00144feabdc0.html#axzz2v0CuP9Lx.
\end{thebibliography}

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 \textit{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, while it was processed by intelligence agents.\footnote{See The Guardian’s interactive site on the Snowden files, \url{http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1}.} 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. The international companies, including BT and Vodafone Cable, responded to criticism of the practice by stating that they are obliged to hand over user data under UK and European Union law.\footnote{James Ball, Luke Harding & Juliette Garside, “BT and Vodafone among telecoms companies passing details to GCHQ,” The Guardian, August 2, 2013, \url{http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq}.}

In October 2013, the parliamentary Intelligence and Security Committee launched an inquiry into the extent and scale of mass surveillance undertaken by Britain’s spy agencies.\footnote{Rowena Mason, “Top web firms urge more transparency over UK requests for user data,” The Guardian, October 18, 2013, \url{http://www.theguardian.com/uk-news/2013/oct/17/uk-gchq-nsa-surveillance-inquiry-snowden}.} The UN also announced an investigation into the surveillance powers of both US and UK intelligence agencies.\footnote{Nick Hopkins & Matthew Taylor, “Edward Snowden revelations prompt UN investigation into surveillance,” The Guardian, December 2, 2013, \url{http://www.theguardian.com/world/2013/dec/02/edward-snowden-un-investigation-surveillance}.} Internet companies like Facebook, Microsoft, Google, Twitter, and Yahoo submitted a memorandum to the UK parliament Home Affairs Committee calling for greater transparency about government requests for user data.\footnote{Rowena Mason, “Top web firms urge more transparency over UK requests for user data.”}

In February 2014, the \textit{Guardian} revealed the existence of another controversial GCHQ surveillance program codenamed Optic Nerve. The program, which dated from at least 2008, indiscriminately collected bulk still images from Yahoo webcam chats until 2010, including substantial quantities of sexually explicit communications. These images were saved to agency databases regardless of whether individual users were intelligence targets.\footnote{Spencer Ackerman & James Ball, “Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ,” The Guardian, February 28, 2014, \url{http://www.theguardian.com/world/2014/feb/27/gchq-nsa-surveillance-surveillance-privacy-yahoo}.} The report led to renewed calls for a review of surveillance laws and practices.\footnote{“Has GCHQ taken a photo from your webcam?” Big Brother Watch (blog), February 28, 2014, \url{https://www.bigbrotherwatch.org.uk/home/2013/02/gchq-nsa-webcam-images.html}; Glyn Moody, “Finally: Senior UK Politicians Start To Call For Review Of GCHQ’s Spying Activities,” TechDirt, March 5, 2014, \url{http://www.techdirt.com/articles/20140304/035808264222/final-politicians-start-to-call-review-gchqs-spying-activities.shtml}.}
Various legislative measures authorize surveillance, including RIPA. 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.

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. However, since the UK’s fiber-optic network often routes domestic traffic through international cables, this provision essentially legitimizes the GCHQ’s ability to conduct widespread surveillance over most, if not all UK citizens.

At the same time, the arrangement allows GCHQ to pass on information to its US counterparts in the NSA regarding US citizens, thereby bypassing American restrictions on domestic surveillance. Documents revealed that the US 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.

In the last year, 514,608 requests for communications data were submitted by public authorities as a whole, down from 570,135 in 2012, while 2,760 lawful intercept warrants were issued, a 19 percent decrease from 2012. The Interception Communications Commissioner undertook a detailed investigation of statutory functions performed by his office—namely overseeing interception requests—after criticism following Snowden’s revelations, and is investigating whether this number of applications amounts to a “significant institutional overuse” of interception agencies’ power. In 2013, 970 communications data errors were reported, leading to 6 separate incidents in which law enforcement agencies acted upon inaccurate data. While the majority of the errors had no serious consequences, in seven of these cases, this led to what the commissioner called “very significant consequences” for involved citizens. The commissioner also expressed his belief that GCHQ and other interception agencies and departments he oversees “do so lawfully, conscientiously, effectively and in the national interest.”

While the UK government has similarly asserted that its surveillance programs are lawful,\(^{150}\) the GCHQ surveillance leaks have led to concerns about how proportionate and justified these methods are. There have also been questions about whether RIPA, which was drafted almost 15 years ago, was ever intended for the purposes to which it is being put,\(^{151}\) and whether reports such as those produced by the interception commissioner are sufficiently transparent.\(^{152}\) Privacy advocates have criticized the tactics as “blanket surveillance,” lacking judicial oversight and undermining the rights guaranteed in Article 8 of the ECHR.\(^{153}\) Some commentators said the British public appeared somewhat apathetic about the revelations.\(^{154}\)

In terms of data protection mechanisms, regulations to implement the 2006 EU Data Retention Directive were adopted in 2009.\(^{155}\) 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.\(^{156}\) In April 2014, however, the European Court of Justice struck down the EU directive as a serious breach of fundamental rights such as privacy.\(^{157}\) 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.\(^{158}\) The UK Data Retention and Investigatory Powers Act requires telecommunication companies to retain users’ metadata for up to 12 months. Academics, journalists, and privacy advocates criticized the legislation for maintaining powers that were struck down by the European court.\(^{159}\) The new act was framed as a temporary fix and will expire at the end of 2016.

In some limited cases, the government uses extrajudicial means to intimidate or pressure users into taking down content. For instance, police reportedly went to the house of a blogger to ask that he...

---


remove tweets related to the Euroscptic UK Independence Party (UKIP), after a counsellor from the party had complained. The blogger, Michael Abberton, is a member of the Green party. The actions reportedly had no legal basis, as the tweets were not abusive or illegal, leading to complaints by Abberton and a member of parliament.  

The Guardian has been investigated for allegedly damaging the UK’s intelligence services and thereby aiding terrorists through its print and online publications of surveillance leaks. The investigation involved police demands to access source material, a police raid of the Guardian’s London offices, and the threat of legal action by the government. In July 2013, GCHQ agents oversaw the destruction of hard drives that contained secret files detailing surveillance activity in a bid to prevent reporting of the leaks from London, despite copies of the material existing outside of the country. No justification has been provided for the allegation that the newspaper’s actions put British national security at risk. Alan Rusbridger, the Guardian’s editor, was called to testify before the governments’ Home Affairs Select Committee in December 2013, where he justified the publication of Snowden’s leaks as being in the public interest. In August 2013, David Miranda, was detained and questioned for nine hours at London’s Heathrow airport while carrying materials belonging to his partner, journalist Glenn Greenwald, who wrote many of the Snowden stories. Various items in his possession were confiscated. The High Court later ruled that his detention was legal under the Terrorism Act.  

There have been numerous incidents of cyberattacks in the UK over the past few years. Apart from intrusions for fraud and other criminal purposes, activist hacking groups have targeted both commercial and government bodies. In October 2013, British citizen Lauri Love was arrested for allegedly hacking into US government computers, although he was later released on bail without charge. Whether he will be extradited to the US to face charges remain to be seen.

---

United States

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>1</td>
<td>2</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>17</td>
<td>19</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 312 million
Internet Penetration 2013: 84 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: No
Press Freedom 2014 Status: Free

Key Developments: May 2013 – May 2014

- In January 2014, a federal appeals court struck down regulations on net neutrality, raising new concerns about discriminatory treatment of content (see Obstacles to Access).

- Self-censorship among journalists and writers reportedly increased due to an awareness of the potential threats to anonymity posed by surveillance of online communications (see Limits on Content).

- Revelations about NSA surveillance continued as more documents were leaked, including reports in September 2013 that the NSA had been working to undermine and circumvent online encryption tools (see Violations of User Rights).

- Advocates and lawmakers continued to push for legal reform of the Electronic Communications Privacy Act, which would require the government to obtain a warrant in order to compel online service providers to disclose private communications (see Violations of User Rights).
Introduction

Access to the internet in the United States remains relatively free compared with the rest of the world. Users face few restrictions on their ability to access and publish content online. The courts have consistently held that federal and state constitutional prohibitions against government regulation of speech apply to material published on the internet. The law also protects online service providers from liability for infractions committed by their users, a policy that fosters business models that permit open discourse and the free exchange of information.

The future of net neutrality in the United States remains uncertain, with the current discussion centered on regulatory safeguards that protect against conduct by internet service providers (ISPs) favoring some internet traffic over others. In January 2014, a court struck down the Open Internet Rules that had been adopted by the Federal Communications Commission to protect net neutrality. As a result, there are currently no legal protections for net neutrality in place. In May 2014, the FCC sought comment on a new regulation that left open the possibility of allowing content providers to strike deals with ISPs for preferential treatment, sparking significant mobilization from a range of stakeholders who urged the FCC to protect net neutrality.

Over the last year, a series of secret documents leaked to major news outlets revealed that the National Security Agency (NSA) is conducting widespread surveillance of American citizens and people around the world. Advocates and academics argue that such surveillance has a chilling effect on writers, human rights activists, religious minorities, and ordinary citizens. Additionally, leaked documents showed that the NSA had been developing programs to crack the security of anonymizing tools such as Tor and other encryption programs. Civil society groups and technology companies have lobbied for surveillance reform, and legislation is moving in Congress that includes a number of provisions to increase transparency and protect individuals’ right to privacy with regard to data and online communications.

Additionally, advocates and lawmakers continue to fight for reform of the Electronic Communications Privacy Act (ECPA), an outdated law that governs how government officials can access private communications through online service providers. Designed for the state of technology in 1986, the law allows for electronic mail to be obtained by the government under a standard weaker than that applicable to postal mail. ECPA reform, if passed, 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.

6 For more on ECPA, see: http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C2968A163.
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 network infrastructure. This model has been questioned by observers who have warned 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. Observers have cautioned that without effective net neutrality regulations (discussed in greater detail below), the dominant companies may decide not to continue carrying internet traffic in a content-neutral fashion.

Although the United States is one of the most connected countries in the world, it has fallen behind several other developed countries in terms of internet speed, cost, and broadband availability. As of 2014, approximately 87 percent of all Americans used the internet at least occasionally at home or work, but only 70 percent of adults had high-speed broadband connections at home as of September 2013. While the broadband penetration rate is high by global standards, it puts the United States significantly behind countries such as Switzerland, the Netherlands, Denmark, and South Korea. Lack of high-speed internet access is especially prevalent in rural areas, where low population densities make it difficult for private companies to justify large investments in network infrastructure. Wired broadband service is not yet available to 7 percent of U.S. residents, mostly in rural counties. A June 2013 Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA) report indicated that 14 percent of rural residents in the United States lack access to fixed broadband. However, mobile broadband is increasingly available to those living in rural areas.

8 According to a study by the Organization for Economic Cooperation and Development (OECD), as of June 2013 the United States was ranked 7th among the OECD member countries in terms of mobile wireless broadband subscriptions per 100 inhabitants, and was ranked even lower, at 16th, on fixed-line broadband penetration. See, OECD Broadband Statistics, “OECD Fixed (Wired) Broadband Subscriptions per 100 Inhabitants, by Technology, June 2013,” and “OECD Terrestrial Mobile Wireless Broadband Subscriptions per 100 Inhabitants, by Technology, June 2013,” accessed May 12, 2014, http://www.oecd.org/sti/broadband/1d-OECD-WiredWirelessBB-2013-06.xls.
United States

Senior citizens, Spanish-speakers, adults with less than a high school education, and those living in households earning less than US$30,000 annually are the groups least likely to use the internet. In a survey conducted by the Pew Internet and American Life Project, when asked why they do not use the internet, many nonusers said they did not see the internet’s relevance in their lives. They also cited factors such as usability and price as key deterrents. Only about 17 percent of nonusers said they knew enough about technology that they could use the internet on their own.

Mobile devices have become nearly ubiquitous in the United States, with 90 percent of adults owning a mobile phone and 58 percent of adults owning a smartphone. Further, 68 percent of adults access the internet through mobile devices, such as smartphones or tablets. Young adults, minorities, those with less than a college education, and those with lower household incomes are the most likely to say that a phone is their primary source of internet access. 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.

No single agency governs the internet in the United States. The Federal Communications Commission (FCC), an independent agency within the executive branch, is charged with regulating radio and television broadcasting, all interstate communications, and all international telecommunications that originate or terminate in the United States. Although the FCC is not specifically tasked with regulating the internet or ISPs, it has claimed jurisdiction over some internet-related issues. Other government agencies, such as the 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.

The United States is home to a thriving communications start-up community where innovators and entrepreneurs regularly offer new technological tools at no monetary cost to the public. Popular web applications such as Twitter, the video-sharing site YouTube, the social-networking site Facebook, and international blog-hosting services such as WordPress are all freely available.

While many broadband service providers operate in the United States, five of them—Comcast, AT&T, Time Warner, and Verizon, and CenturyLink—control 70 percent of the market. These companies serve a combined 60 million customers and own the majority of network cables and

other infrastructure. Until 2005, U.S. telephone companies were required to grant other ISPs “nondiscriminatory” access to their wire networks in order to ensure open retail-level competition and optimal service for consumers. However, in 2005, the FCC embraced an aggressive deregulation agenda and freed network owners from any obligation to lease their lines to competing ISPs. The proponents of deregulation claimed that this step would provide more incentive for large cable and telephone companies to further develop and upgrade their networks, while opponents claimed that it would lead to higher prices, fewer options for consumers, and worse service. Broadband speeds have increased, but a majority of Americans remain limited to two or fewer options when choosing a broadband provider offering at least 6 Mbps for downstream speeds and 1.5 Mbps for upstream speeds.

Over the last decade, policymakers in the United States have debated the concept of net neutrality, according to which network providers must treat all content, websites, and platforms equally when managing data traffic. Supporters of the principle argue that without it, ISPs would effectively be able to block certain content and applications, or give preferential treatment to some content providers for a fee, a practice that could place limitations on citizens’ access to information and online services.

Although concerns about net neutrality began emerging in the early 2000s, the issue gained widespread attention in 2007 when FCC investigators found that Comcast, a cable-television company and major ISP, had begun slowing down and blocking certain types of peer-to-peer file-sharing traffic. After a long court battle on the issue, a federal appeals court sided with Comcast in April 2010 and overturned the FCC’s ruling against the company. The decision also found that the FCC did not have the authority to regulate ISPs under the legal framework the agency had cited, challenging its ability to protect consumers on the internet.

In December 2010, the FCC issued a compromise ruling on net neutrality (known as the Open Internet Rules) that required fixed-line service providers not to block access to, or unreasonably discriminate against, lawful websites, applications, devices, or services. The rules for wireless broadband providers were much more limited, restricting only some types of blocking and saying nothing about discrimination. Under separate FCC licensing rules covering the operation of a particular range of radio communication frequencies, some wireless carriers are barred from discriminating among devices and applications, but these rules are not universally applied. In 2011, advocates filed a complaint with the FCC alleging that Verizon had violated these licensing rules by demanding that certain applications (specifically, applications that enable a mobile device to create a wireless “hotspot,” essentially sharing its connection with other devices) be removed from Google’s

---


application store. In 2012, Verizon settled this complaint with the FCC, agreeing that the company would not restrict the availability of such applications.\textsuperscript{25}

In a decision issued in January 2014 (\textit{Verizon v. FCC}), the federal court of appeals in Washington DC struck down the Open Internet Rules for both fixed and mobile access providers.\textsuperscript{26} The court ruled that the FCC does have some jurisdiction over broadband providers under a statute intended to ensure the rapid deployment of high-speed communications capability. It also found, however, that the FCC was prevented from imposing a nondiscrimination obligation on providers of broadband internet access due to its prior decisions on the regulatory classification of broadband. On May 15, 2014, the FCC opened a new consultation on the issue, but there are currently no legal protections for net neutrality in place, and it is unclear how robust and legally stable the FCC’s next attempt will be.\textsuperscript{27} The rule proposed by the FCC in May was criticized by many net neutrality proponents for not going far enough to preserve open, non-discriminatory access to content of users’ choice. But, there is strong opposition in Congress and among internet service providers to the idea put forth by some net neutrality advocates that the FCC should reclassify broadband as a service that could legally be subjected to a nondiscrimination regime.\textsuperscript{28}

\section*{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. At the same time, recent revelations about the extent of government surveillance of online communications have led some to report an increase in self-censorship.

Although the government does not restrict any political or social content, legal rules that apply to other spheres of life have been extended to the internet. For example, concerns over copyright violations, child pornography, protection of minors from harmful or indecent content, harassing or defamatory comments, publication of confidential information, 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


\textsuperscript{26} \textit{Verizon v. FCC}, 740 F.3d 623 (D.C. Cir. 2014).

\textsuperscript{27} Notice of proposed rulemaking available at \url{http://www.fcc.gov/document/fcc-launches-broad-rulemaking-protect-and-promote-open-internet}.

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, such as the Child Online Protection Act of 1998 (COPA), but they have been overturned by courts due to their ambiguity and potential infringements on the First Amendment of the U.S. Constitution, which protects freedoms 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.  

In addition to restricting access to universally illegal content such as child pornography, 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 and sites that sell counterfeit goods. These seizures have been criticized as overly secretive and lacking in due process; for example, ICE seized the domain name of a legitimate hip-hop music site in November of 2010 and refused to return it for an entire year. The decision to withhold the domain was based on sealed court proceedings to which the owners of the domain were not allowed access. In August 2012, three members of Congress wrote a letter to the U.S. Attorney General raising concerns about whether ICE procedures give websites meaningful due process. However, 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, called “Project Cyber Monday IV,” resulted in the seizure of 297 domains.

---

29 Treating domain names as property subject to criminal forfeiture, 18 U.S.C. 2253.
The activities of WikiLeaks, which in 2010 published several tranches of U.S. government material that was leaked by U.S. Army intelligence analyst Chelsea Manning (formerly Bradley Manning), triggered a serious debate about the use of the internet to publicize sensitive or classified government documents.36 WikiLeaks faced the cut-off of service by non-government entities, including Amazon’s data storage service37 and EveryDNS, Wikileaks’ domain name service provider.38 While these and other companies that severed ties with WikiLeaks claimed to be acting independently and without government influence, their decisions came amid fierce public criticism of WikiLeaks by executive branch officials and prominent members of Congress.39 Manning pleaded guilty to some charges, was convicted of others and received a lengthy sentence in August 2013. According to a Washington Post article published in November 2013, government officials reported that while the grand jury investigation of Wikileaks is technically ongoing, it is unlikely that the organization’s leader, Julian Assange, will face charges in the United States.40 Likewise, the Attorney General has said that the U.S. 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.”41

The legality of online gambling is another topic of debate in the United States. Online gambling is governed by a patchwork of state and federal laws. In 2011, the Justice Department delivered a legal opinion clarifying the scope of the Wire Act of 1961, which opened the door for states to legalize a number of forms of gambling, including online poker.42 Following the opinion, Nevada, New Jersey, and Delaware legalized online gambling within their borders. Other states are considering similar legislation.43 Some elected officials at the federal level oppose this trend. In March 2014, Senator Lindsey Graham and Congressman Jason Chaffetz introduced a bill that would reverse the Justice Department's 2011 interpretation. As of May 2014, the bill had not progressed out of committee.44

In November 2013, the free expression and literature advocacy group PEN America released the results of a survey showing that the NSA surveillance revelations had resulted in increased self-
censorship among writers. Since the revelations began in June 2013, 28 percent of respondents reported having altered or avoided social media activities, 24 percent reported deliberately avoiding certain topics in phone or email conversations, and 16 percent reported avoiding writing or speaking about a particular topic. Additionally, Human Rights Watch conducted a survey of journalists and lawyers revealing the degree to which NSA 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.

The internet plays a significant role in civic activism in the United States, and the growth of the blogosphere and citizen journalism has changed the ways in which many people receive news. Blogs and electronic media outlets reporting from various points on the political spectrum now have greater readership than most printed periodicals. Nearly all nongovernmental organizations and causes have a presence on the internet and use it for advocacy and social mobilization. Email campaigns, online petitions, and YouTube videos have been instrumental in organizing protests, lobbying government bodies, and educating the public.

In 2011, technologists, digital rights advocates, companies such as Google and Mozilla, and the internet community at large came together to voice resounding opposition to two bills, the PROTECT IP Act (PIPA) and the Stop Online Piracy Act (SOPA), largely using online tools. SOPA and PIPA sought to target websites outside of the United States that host material allegedly infringing on U.S. copyrights. The bills would have permitted the Attorney General, with little judicial review, to seek orders directing ISPs to block access to domain names of sites allegedly dedicated to infringing activity, even if sites also contained lawful content. SOPA and PIPA threatened to suppress unquestionably legal speech and posed a threat to the infrastructure of the internet. Online mobilization against SOPA and PIPA was unprecedented: 10 million signatures to petitions, 4 million emails to legislators, and 115,000 sites blacking out or going dim in protest. In response to these efforts and internal concerns, members of Congress withdrew the bills from consideration. Political activity is increasingly moving online. According to a 2013 survey by the Pew Center’s Internet and American Life Project, 34 percent of adults had recently contacted a government official or spoken out in a public forum using online methods. In addition, 39 percent of American adults had taken part in a political activity using a social networking site like Facebook or Twitter in the 12 months preceding the survey. Groups looking to encourage political action frequently use online tools to contact Americans; in the Pew survey, 21 percent of email users indicated that they regularly receive calls to action on social or political issues by email. In addition, political candidates and

---


elected officials at the local, state, and federal level increasingly use email, mobile apps, and online content to garner support and keep their constituents engaged.

Violations of User Rights

The United States has a robust legal framework that supports free expression rights both online and offline, and the United States 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.

The U.S. Constitution includes strong protections for free speech and freedom of the press. In 1997, the U.S. Supreme Court held that internet speech was entitled to the highest form of protection under the constitution, and 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.49

There have been 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. In 2012, federal authorities issued a subpoena to the microblogging service Twitter, requesting information from the Twitter accounts of Chelsea Manning (formerly Bradley Manning), Julian Assange, and others associated with WikiLeaks. With the subpoena came a gag order compelling Twitter not to disclose this information to anyone, including the users in question. Twitter attorneys successfully challenged the gag order in court and were able to notify users before disclosing their information to government officials.50

In March 2014, a U.S. magistrate judge in Washington D.C. took an unusual step in a case involving secret grand jury subpoenas. The judge issued orders in two cases denying Justice Department requests for gag orders that would have prohibited Twitter and Yahoo from telling anyone, including the affected customers, that the companies had received demands for disclosure of user information. The judge specified that gag orders would not be granted until the companies had an opportunity

to respond. However, a district court judge set aside the magistrate’s orders. The case illustrates the uneasiness among at least some federal magistrates (low level judges who handle most government applications for surveillance and access to communications data) over the exercise of the government’s surveillance powers.

In another concerning case regarding government access to information, the Associated Press (AP) reported in May 2013 that, as part of a national security leak investigation, the U.S. Justice Department subpoenaed and gained access to two months of phone records for several reporters following AP coverage of a failed bomb plot in Yemen. Justice Department guidelines specify that, in the course of an investigation, requests for journalists’ records should be “as narrowly drawn as possible,” and that investigators should attempt to obtain records directly from journalists on a voluntary basis, when possible. The Associated Press has since reported that the government’s actions have had a chilling effect on sources, discouraging even long-standing informants from speaking with the AP. In February 2014, the Attorney General signed a set of guidelines that limit the circumstances under which government may access journalists’ records, but the document does not prohibit the practice entirely.

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.\(^{60}\) As of May 2014, the bill remains stalled in the House Judiciary Committee.

In August 2011, public transit authorities in San Francisco suspended mobile phone service in several underground stations of the Bay Area Rapid Transit (BART) system in an effort to impede planned demonstrations regarding the fatal shooting of a man by BART police the month prior. Numerous digital rights advocates and First Amendment scholars called the decision a violation of BART passengers’ First Amendment rights.\(^{61}\) Following the incident, various civil liberties groups filed an emergency petition with the FCC requesting that the agency declare the BART shutdown a violation of the Communications Act.\(^{62}\) In early 2012, the FCC issued a call for public comment on the issue, but as of mid-2014 the agency had not yet taken further action on the subject.\(^{63}\) In December 2011, BART adopted a policy outlining the circumstances under which it could shut down service; the policy did not require prior judicial approval, but had it been in place, it would not have allowed for the August 2011 shutdown.\(^{64}\) In September 2013, the state of California adopted legislation requiring state and local officials to obtain a court order before interfering with electronic communications systems used by the public. Certain emergency situations are exempted from this rule, which went into effect on January 2014.\(^{65}\)

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,\(^{66}\) 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.\(^{67}\) In April 2011, the Obama administration launched the National Strategy for Trusted Identities in Cyberspace (NSTIC). The stated goal of the effort is to ensure 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. The plan specifically endorses anonymous online speech.

While there are no legal restrictions on anonymous communication online, there is evidence to suggest that the intelligence community in the U.S. has been working to undermine the security of anonymizing tools. 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), as well as efforts to undermine international technical standards for encryption.

Laws that protect internet communications from government monitoring are complex. While in transit, the contents of internet communications are protected from government intrusion by constitutional rules against unreasonable searches and seizures. The courts, however, have held that transactional data about communications—data showing who is communicating with whom and when—is not protected by the constitution.

Under a set of complex statutes, law enforcement and intelligence agencies can monitor communications and access stored information under varying degrees of oversight as part of criminal or national security investigations. In criminal probes, law enforcement authorities can monitor the content of internet communications in real time only if they have obtained an order, issued by a judge, under a standard that is actually a little higher than the one established by the constitution for searches of physical places. The order must reflect a finding that there is probable cause to believe that a crime has been, is being, or is about to be committed. 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. However, the 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. As of mid-2014, 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 storage.

---

74 United States v. Warshak, 09-3176, United States Court of Appeals for the Sixth Circuit.
75 Ibid.
Following the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act, which expanded some of the government's surveillance and investigative powers in cases involving terrorism as well as in ordinary criminal investigations. Three expiring provisions of the PATRIOT Act—including the government's broad authority to conduct roving wiretaps of unidentified or "John Doe" targets, to wiretap "lone wolf" suspects who have no known connections to terrorist networks, and to secretly access a wide range of private business records with court orders issued on a broad standard (Section 215)—were renewed for an additional four years in May 2011.

However, starting in June 2013, it became clear that the issues debated in connection with the PATRIOT Act were only the tip of the iceberg in relation to U.S. government surveillance. That month, the Guardian, the Washington Post, and other news outlets revealed a series of secret documents leaked by former National Security Agency (NSA) contractor Edward Snowden that provided new information (and raised many new questions) about surveillance activities conducted by the U.S. government.

Leaked documents indicated that the Foreign Intelligence Surveillance Court (FISA Court) had interpreted Section 215 of the PATRIOT Act to permit the FBI to obtain orders that compel the largest telephone carriers in the United States (Verizon, AT&T, Sprint, and presumably others) to provide the NSA with records of all phone calls made to, from, and within the country on an ongoing basis. These billions of call records include numbers dialed, length of call, and other "metadata." Data are gathered in bulk, without any particularized suspicion about an individual, phone number, or device. Without approval from the FISA Court or any other judicial officer, NSA analysts conduct queries on this data, generating contact chains that show the web of connections emanating from a single phone number suspected of being associated with terrorism.

Leaks also revealed new details about programs authorized by Section 702 of the Foreign Intelligence Surveillance Act. Section 702 allows the NSA to conduct surveillance of people who are not U.S. citizens and who are reasonably believed to be located outside the United States in order to collect “foreign intelligence information.”\(^ {83}\) Under a program called “PRISM,” the NSA has been compelling at least nine large U.S. companies, including Google, Facebook, Microsoft and Apple, to disclose content and metadata relating to emails, web chats, videos, images, and documents.\(^ {84}\) Also under Section 702, the NSA taps into the internet backbone for “collection of communications on fiber cables and infrastructure as data flows past.”\(^ {85}\) Although these programs are targeted at persons abroad, the NSA is able to retain and use information “incidentally” collected about U.S. persons.

Meanwhile, Executive Order 12333\(^ {86}\) offers the legal basis for additional surveillance programs outside the scope of FISA. Executive Order 12333 specifically addresses surveillance conducted abroad that targets non-U.S. persons (those who are not U.S. citizens or permanent resident aliens) located outside the United States. There is limited public information about how Executive Order 12333 has been interpreted by government officials, but the surveillance procedures issued under the Executive Order are designed to provide protections to U.S. citizens and residents, not to others who may be put under surveillance.\(^ {87}\) The Executive Order authorizes surveillance of people outside the U.S. on a very broad scale: the “foreign intelligence information” that can be sought with surveillance includes information about “the capabilities, intentions, or activities” of foreign organizations or persons.

Surveillance activities likely conducted under Executive Order 12333 authority include: bulk collection of location data from cell phones;\(^ {88}\) bulk collection of text messages;\(^ {89}\) bulk collection of contact lists from personal email and instant message accounts;\(^ {90}\) collection of mass amounts of data flowing between data centers of major technology companies such as Google and Yahoo;\(^ {91}\) and collection of user data available from mobile phone applications, including geographic data, address

---

\(^ {83}\) 4 Sec. 702 was adopted in 2008 as part of the FISA Amendments Act, Pub. L. 110-261, https://www.govtrack.us/congress/bills/110/hr6304


\(^ {86}\) The text of Executive Order 12333 is available at: https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf


\(^ {90}\) Barton Gellman and Ashkan Soltani, “NSA Collects Millions of E-mail Address Books Globally,” the Washington Post, October 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5b5-34f2-11e3-8c6-76edd8d22d8f_story.html.

books, “buddy lists,” and telephone logs. Critics assert that the secret NSA programs violate the Fourth Amendment, which protects people inside the United States (citizens and non-citizens alike) from unreasonable search and seizure, as well as human rights enshrined in international agreements. The Snowden leaks have prompted significant mobilization by civil society and companies.

Over the last year there have been some positive developments. In January 2014, the president announced that he intended to end the bulk collection of telephony metadata. As of May 2014, however, the program was still operating, as Congress debated legislation to end it. In January, the president also issued a policy directive that put in place important new restrictions on the use of information collected in bulk for foreign intelligence purposes. The restrictions apply to communications data regarding all persons, “whatever their nationality and regardless of where they might reside.” However, the restrictions do not apply to data collected under Section 702 because it is not considered a bulk collection program.

The Communications Assistance for Law Enforcement Act (CALEA) 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. The FBI has repeatedly requested that the law be expanded to impose design requirements on online communications tools such as Gmail, Skype, and Facebook. 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. Following the leaks about NSA surveillance, focus in Washington shifted away from CALEA II, but it is possible that similar proposals will emerge in the future.

---

94 See for example https://www.reformgovernmentsurveillance.com/.
98 During the PCLOB’s March 19 public hearing on Section 702, government officials maintained that surveillance pursuant to Section 702 is not bulk collection and that this rule does not apply to such surveillance. See generally, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, March 19, 2014, http://www.pclob.gov/Library/20140319-Transcript.pdf.
99 The FCC does not classify Skype as an “interconnected VoIP” service.
Law enforcement agencies have also used open, public websites and social media platforms to monitor different groups for suspected criminal activity. One notable example that generated controversy was an initiative by the New York Police Department (NYPD), uncovered in February 2012, to monitor Muslim student groups at various universities in the northeastern United States. The Associated Press reported that, from 2006 onward, the NYPD Cyber Intelligence unit had 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.102 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. Civil liberties advocates welcomed this step but warned that other NYPD units may still be using discriminatory practices.103

Like most other countries, the United States faces the growing challenge of addressing cyberattacks conducted by both state and non-state actors. In response to concern about cybersecurity threats, President Obama produced an executive order in 2013 recognizing the need for improved cybersecurity measures and calling for a new “Cybersecurity Framework” to address security threats.104 The executive order directed agencies to “ensure” that privacy and civil liberties protections are incorporated into their cybersecurity activities, and it specified that such protections shall be based on the Fair Information Practice Principles, an internationally recognized framework for privacy protection. At the same time, the U.S. military admitted that it is developing the ability to carry out offensive cyberattacks.105 The documents leaked by Edward Snowden included a Presidential Policy Directive describing U.S. “Offensive Cyber Effects Operations (OCEO).”106

China is one focal point of the cybersecurity discussion, especially following a report by computer security firm Mandiant stating that many attacks against U.S. organizations, companies, and government agencies appear to have originated in an office of the Chinese People’s Liberation Army in Beijing.107 Following tense exchanges on the issue in 2013, the United States attempted to open a dialogue with China about cybersecurity. In early 2014, U.S. officials held a briefing for Chinese military leadership on the Pentagon’s cybersecurity tactics and policy, including both offensive and defensive programs. The purpose of the briefing was to build trust and encourage reciprocity from the Chinese government.108

In March 2014, the United States government reported that it had notified 3,000 companies over the last year that their technology systems were under attack. This number represents only a small fraction of all cybersecurity threats to U.S. businesses and their customers but points to the seriousness of the problem.109 One of the most significant attacks in 2013 targeted the financial services industry, using denial-of-service attacks to reduce availability of networks and services.110 While some attacks target whole networks or industries, others focus on individual internet users. For example, the Ethiopian government allegedly installed surveillance spyware on the computer of a U.S. citizen living in Maryland in order to monitor his activity over a period of months. With the assistance of the Electronic Frontier Foundation, the man is suing the Ethiopian government in a United States court for illegal wiretapping.111 Similar surveillance software appears to be used by governments around the globe.112


112 See for example: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/
Uzbekistan

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>20</td>
<td>20</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>30</td>
<td>31</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>78</td>
<td>79</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 30 million

Internet Penetration 2013: 38 percent

Social Media/ICT Apps Blocked: Yes

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- In February 2014, President Karimov signed a resolution granting Uzmobile the legal status of a “national mobile phone provider,” causing concerns that this will reduce competition over the next few years and make the domestic market of mobile communications more susceptible to state control (see Obstacles to Access).

- The state-owned national telecommunications operator, Uztelecom, has become the sole ISP providing internet access in libraries, schools, universities, and youth and cultural institutions (see Obstacles to Access).

- One internet user was sentenced to eight years of imprisonment and two photojournalists received high fines for their online activities (see Violations of User Rights).

- Surveillance in internet cafes and public internet access points has increased due to a new regulation requiring cafe owners to install surveillance cameras and log user activities (see Violations of User Rights).
Uzbekistan

Introduction

Since May 2013, Uzbekistan’s government has taken further measures to intensify its grip over internet connectivity. The state-owned telecommunications carrier, Uztelecom, continues to monopolize the country’s internet access, making it a highly profitable state enterprise with no liberalization in sight. In July 2013, the government revoked the right of private ISPs to provide internet access in libraries, schools, universities, and youth and cultural institutions, granting this right exclusively to Uztelecom. Competitive conditions have also deteriorated for mobile phone companies, in particular for the two foreign GSM operators that continue to provide mobile and broadband services after the government expropriated a subsidiary of the Russian MTS last year. Citing concerns over the reliability, stability, and adaptability of mobile networks to information security concerns, the government has taken steps transform Uztelecom’s CDMA operator, Uzmobile, into a national mobile phone operator with a target of 8 million subscribers by the end of 2017. These developments raised concerns about an intensification of state censorship and surveillance on telecommunications and mobile broadband networks.

The environment for internet users’ rights in Uzbekistan remains one of the most restrictive in Central Asia. The Uzbek authorities block access to a wide range of websites and control content available at cultural and educational institutions through the intranet, ZyioNET, and the national search engine at www.uz. The government also employs extensive surveillance measures to monitor online activity and frequently uses trumped-up charges to target individuals who publish material online that is deemed antithetical to the government’s interests. In 2013, one internet user was sentenced to eight years of imprisonment for establishing online communications with an exile opposition group via Skype, Facebook and the Russian social network Odnoklassniki.ru, and for distributing materials on the group’s orders that were perceived as violating the constitutional order.

Stringent control of the internet is expected during the parliamentary elections in December 2014 and the presidential elections in 2015. Already in the fall of 2013, political turmoil around the president’s daughter, Gulnara Karimova, and her active use of Twitter, presumably led to intensified control of social networks by the National Security Service (NSS).

Obstacles to Access

The internet penetration rate in Uzbekistan reached over 38 percent in 2013, compared to about 37 percent in 2012 and 9 percent in 2008, according to the International Telecommunication Union (ITU).\(^1\) Official Uzbek sources reported in April 2013 that 9.8 million Uzbek people had access to the internet through the use of a personal computer at home or at work.\(^2\) According to the latest available official data, announced by President Karimov in his speech on democratic reforms and civil so-


Online society in Uzbekistan in December 2013, there were 7.1 million people with internet subscriptions. On December 31, 2013, the government adopted the resolution “On the Introduction of the System to Evaluate the ICT Development in Uzbekistan” to improve the methods for calculating ICT data.

Digital divides exist between the capital 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 the FTTB and WiMAX broadband connectivity. The lowest internet penetration rate is in the semi-autonomous republic of Karakalpakstan—a home to the Karakalpak, Kazakh, and Uzbek ethnic groups. The usefulness of ICT facilities, especially in rural and remote areas, still depends on a stable electricity supply to the telecommunications infrastructure. 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 306,300 internet users had a fixed-broadband subscription in 2013. The construction of the fiber-optic network (FTTx) in Uzbekistan required US$9 million in Uzbek and Chinese investments from 2013-2014. By January 2014, the fibre optic network was 2,100 km long. The government goal is to have 110,000 ports for broadband connection across the country by 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 organs of local governance (hokimiat) at the regional and city levels in Uzbekistan by the end of 2013. 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.

---

11 See Resolution of the President RU No. ПП-1920.
March 2014 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.\textsuperscript{12}

Public access points such as internet cafes remain popular, particularly among young 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.\textsuperscript{13} Reportedly, since 2011, students are also not allowed to visit internet cafes between 8:30 a.m. and 7:00 p.m.\textsuperscript{14} 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.\textsuperscript{15}

In a new attempt to limit and control internet access, in July 2013, the government allowed the state-owned telecommunications operator Uztelecom to serve as the exclusive provider of access to ZiyoNet across these target institutions nationwide.\textsuperscript{16}(Previsously, beginning in 2005, any private ISP could exercise that right on a competitive basis\textsuperscript{17}. 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 1,441,101 UZS (approximately US$650).\textsuperscript{18}

The state-owned JSC Uzbektelecom, established in 2000 and re-branded as “national operator Uzbektelecom” in 2011, owns and operates Uzbekistan’s telecommunications infrastructure under a state license renewable every 15 years. In August 2005, Uzbektelecom took over the internet connectivity functions from the state data transfer network company, UzPAK, that was established in 1999 and presently operates as Uzbektelecom’s subsidiary.\textsuperscript{19} As an upstream ISP, Uzbektelecom requires private ISPs to route and transmit their international traffic through its International Centre for Packet Switching ("Mezdunarodnyi tsentr paketnoyi kommutatsii"). Uzbektelecom sells internet traffic to private ISPs at a wholesale, U.S. dollar-denominated price per 1 Mbps (US$312.58 in December 2013).\textsuperscript{20} Uzbektelecom controls the country’s external internet gateway capacity, which allows the authorities to control access speeds for the entire country, if needed. Uzbektelecom has the technical means to boost speeds

\textsuperscript{13} "О порядке предоставления доступа к сети Интернет в общественных пунктах пользования" [On Adoption of the Terms of Provision of Access to the Internet Network in Public Points of Use], promulgated by Order of the Communications and Information Agency of Uzbekistan No. 216, July 23, 2004, SZRU (No. 30), item 350, at Art. 17 (e).
\textsuperscript{15} Resolution of the President RU “О создании общественной образовательной информационной сети Республики Узбекистан” [On the Establishment of the Public, Educational, and Information Network of the Republic of Uzbekistan], No. ПП-191, 28 September 2005, SZRU (No. 40), item 305, at Art. 4.
\textsuperscript{17} Compare Resolution of the Cabinet of Ministers RU “О дальнейшем развитии информационной сети “ZIYONET” [On the Further Development of the Educational Network “ZIYONET”], No. 52, item 389, at Art. 4 (no longer valid).
\textsuperscript{18} Uzbektelecom, Uzonline internet tariffs as of February 12, 2014, at http://uzonline.uz/ru/services/internet/#life.
\textsuperscript{19} Decree of the President RU „On measures for development of data transfer services and preparation for privatization of JSC „Uzbektelecom”, No. PP-149, August 8, 2005.
Uzbekistan

from the current 10.3 Mbps to 100 Mbps.\(^{21}\) In 2011, the government prohibited private ISPs from bypassing Uztelemcom’s infrastructure of 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 Uztelemcom.\(^{22}\) TAS-IX ISPs are challenged to find the income streams for the investments needed to meet the capacity requirements of their customers.\(^{21}\) Private ISPs provide no traffic limitations to websites hosted within the TAS-IX networks but filter and block content or applications to the same extent as Uztelemcom.\(^{24}\)

Expensive access prices, low 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 TAS-IX and internet access routed via Uztelemcom’s network. On the one hand, Uztelemcom and private ISPs provide free access to the TAS-IX network at a maximum download speed of 2 Mbps to their customers. On the other hand, 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).\(^{25}\)

Uztelemcom remains a leader in the provision of FTTB broadband internet to private households and businesses. However, neither Uztelemcom 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, Uztelemcom 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.\(^{26}\)

According to official statistics, at least eight leading private ISPs have transferred Uztelemcom’s price reductions to their individual subscribers and dropped subscription prices between 15 and 80 percent from 2011 to 2013.\(^{27}\) At the same time, according to the ITU, internet access prices are still prohibitively expensive in comparison to the average household income in Uzbekistan.\(^{28}\) In addition,

\(^{21}\) Uztelemcom, “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/2014/1327/.


\(^{24}\) TAX-IS participating ISP maintain a service to find out whether a website is in the TAS-IX network. See, e.g., ISP TPS, http://www.tps.uz/tasix/.

\(^{25}\) See, e.g., a tariff list from the leading ISP provider TPS, at http://www.tps.uz/tariffs/section/jet (last accessed on April 26, 2013).

\(^{26}\) See tariff “Record-6” as of February 12, 2014, at http://uzonline.uz/ru/services/internet/\#life.


\(^{28}\) 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.”
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.

As of 2013, there were 21.5 million mobile phone subscriptions (a mobile penetration rate of rate of 74 percent) and four operators of mobile communications in Uzbekistan. The smallest numbers of subscribers reportedly belong to two CDMA operators—Uzmobile (a brand of the state-owned Uztelecom) and Perfectum Mobile (owned by the Uzbek company Rubicon Wireless Communication). Two GSM operators—Beeline (owned by the Russian VimpelCom Ltd) and Ucell (owned by the Swedish-Finnish company TeliaSonera)—shared 54 percent and 41 percent of the market, respectively, in 2014.

All four mobile operators offer internet access. Uzmobile offers mobile internet via CDMA-450 networks. Availability of mobile broadband based on 4G/LTE technology remains limited to the capital Tashkent, particularly after the former leading GSM operator Uzdunrobita left the market. Speeds for broadband internet are very low in Uzbekistan compared to international standards. According to Net Index Explorer by Ookla, tests carried out in the capital Tashkent and the city of Chilanzar demonstrate the mobile broadband upload speeds of 0.6 Mbps in May 2012 to 0.5 Mbps in March 2014, with the lowest mark of 0.41 Mbps in July 2013. Akamai reports indicate that the average connection speed in 2013 was approximately 1.96 Mbps. Two leading operators, Beeline and Ucell, offered upload speeds at 1.75 Mbps and 1.49 Mbps in March 2014.

From July 2012 through April 2013, the government took steps to terminate the operations of the leading GSM operator Uzdunrobita (a wholly owned subsidiary of the Russian MTS) that 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. In February 2014, an arbitration proceeding between MTS and Uzbekistan was pending at the International Centre for Settlement of Investment Disputes of the World Bank. As of August 2014, MTS and the government of Uzbekistan had reached an agreement whereby MTS would resume operations in the country through a joint venture with the government, in which the State Committee for Communications, Informatization and Telecom-

---


Uzbekistan

By 2017, competition within the mobile communications market in Uzbekistan may shrink even 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.”

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 by the end of 2017. Earlier, in October 2013, the companies Unitel (Beeline) and Coscom (Ucell) were included into the organizational structure of the telecommunications regulator along with the state-owned Uztelemcom.

In 2013, the disclosure of systematic bribery solicited from foreign mobile companies MTS and TeliaSonera by the president’s daughter, Gulnara Karimova, called attention to the existence of rampant corruption affecting the mobile telecommunications industry in Uzbekistan. Furthermore, regulatory burdens such as the numerous licenses and permissions that mobile phone companies must obtain in bureaucratic and time consuming administrative processes, intricate customs procedures for the import of ICT equipment, and unduly complicated tender conditions hinder their business operations. Late last year, bureaucratic obstacles became particularly burdensome for Beeline amid its network capacity investments to accommodate large inflows of former subscribers of Uzdunrobita. The company experienced problems obtaining permission from the State Inspectorate on Communications to deploy its new 460 mobile phone base stations and to use additional free mobile phone numbers for newly connecting customers. Under the national regulatory regime, a permission issue process for deployment of mobile phone base stations may take up to 24 months, thus, as some observers note, increasing the risk of corruption. An unscheduled tax audit—another popular state measure used to interfere with the activity of private businesses in Uzbekistan—was conducted at Beeline from October to December 2013, though no violations of national law were reported.

38 Resolution of the President RU “Об утверждении обновленной структуры государственного комитета связи, информатизации и коммуникационных технологий Республики Узбекистан” [On the Updated Structure of the State Committee for Communications, Informatization, and Telecommunication Technologies], No. ПП-2058, October 30, 2013, SZRU (2013) No. 44, item 578.
Uzbekistan

The use of mobile technology in schools and universities remains limited. On May 21, 2012, the government adopted a resolution establishing unified rules for the use of mobile phones in all educational institutions of the country. The resolution completely bans the use of mobile phones in the buildings of educational institutions, not only for students but also for teachers and other personnel. According to the resolution, the aim of such measures is to prevent “negative aspects” of the use of mobile phones in educational settings, such as cheating; digital gaming; and the dissemination of materials undermining morals and ethics, promoting a culture of violence, cruelty and pornography, or promoting “reactionary sectarian, pseudo-religious ideology.” Another stated aim, however, is to enable the “education of the youth in the spirit of love to its motherland, respect for national values and those of the humanity, [and] ideas of national independence.” In the past, the government has sporadically ordered the shutdown of text messaging and internet services by mobile operators, particularly during exams.

The government’s control over the internet infrastructure and its influence on mobile phone operators enables it to limit or block connectivity to websites and applications at will, which it appears to have done on several occasions in recent years. In August 2011, individual users and independent news websites reported that the Google search engine and its Russian equivalent, Rambler, were blocked for several days amid a broader increase in blocked websites. Government officials and service providers denied that the disruptions were intentional, but observers suspected that the restrictions were related to the upcoming 20th anniversary of the end of the Soviet era in September 2011 and the government’s fear that it might trigger social media-inspired protests in Uzbekistan.

Apart from these sporadic restrictions, YouTube, Facebook, Twitter, and LiveJournal remained generally available in 2013–2014, though some individual pages were blocked. In March 2012, however, reports emerged that the Uzbek authorities had temporarily blocked LiveJournal out of concern that potential protests could erupt over the results of the Russian presidential elections. The blog-hosting platform Wordpress remained blocked in its entirety during the reported period.

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

---

43 Resolution of the Cabinet of Ministers RU, “О мерах по упорядочению пользования мобильными телефонами в образовательных учреждениях Республики Узбекистан” [On measures to streamline the use of mobile phones in educational institutions of the Republic of Uzbekistan], No. 139, May 21, 2012, SZ RU (2013 No. 21 (S21), item. 229.
44 “Uzbekistan ‘halts mobile Internet, SMS’ for exam day,” AFP, August 2, 2011, http://www.google.com/hostednews/afp/article/AlEqM5jAt_J3V1eB_Homvu0Osp2k3mqMdQ.
Uzbekistan

government’s inner circle regularly denied licenses for unjustifiable reasons. The government has since March 2014, no license to open an internet cafe can be given if the internet cafe premises are located in the basement or semi-basement rooms of multistory buildings.

The State Committee for Communications, Informatization and Telecommunications Technologies (State Committee for CITT) regulates the entire ICT industry in Uzbekistan, including the internet and ISPs. The committee lacks independence and is accountable to the Cabinet of Ministers in the executive branch. The process for appointing members of the committee lacks transparency and is not representative of different stakeholders’ interests. The president appoints and dismisses the committee chairman and first deputy, who are also members of the Executive Board of the national operator Uztelecom, where the committee has the right to manage 51 percent of state shareholdings. Moreover, the Cabinet of Ministers approves members of a committee’s collegium selected from the committee’s top bureaucrats. The collegium coordinates the planning and implementation of the committee’s main activities and appoints the committee’s nomenklatura.

The government maintains direct control over the administration, registration, and use of domain names with the “.uz” top-level domain, which was established in April 1995 and re-delegated to the government in April 2003. Current rules for the assignment, registration, and use of the country’s top-level domain create an obstacle to internet access. The Computerization and Information Technologies Developing Center (Uzinfocom) manages the “.uz” top-level domain. There are seven private ISPs officially authorized to provide registry services in the “.uz” domain zone. 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.

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 related to foreign and domestic 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.

Websites permanently blocked in Uzbekistan do not appear on www.uz, the national search engine of Uzbekistan's government. These websites include any independent news websites with socio-political and human rights-related content on Uzbekistan, including CA-News (Centrasia.ru), Fegananews.com, Harakat.net, Mediauz.ucoz.ru, UzMetronom.com, and Uznews.net. Websites of Uzbek human rights and opposition groups in exile are also blocked. The websites of the international broadcasters BBC (Bbc.co.uk/uzbek), Radio Free Europe/Radio Liberty (Ozodlik.org), Deutsche Welle (Dw.de), and Voice of America (Voanews.com/uzbek) have remained 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.

In February 2013, presumably under pressure of the Uzbek government, administrators of the Russian social-networking site Odnoklassniki.ru removed a web page of the National Movement of Uzbekistan “without the possibility of being restored.” At the time of removal, the Uzbek dissident group that had been established in 2011 had 26,000 “friends” on Odnoklassniki. The official website of the movement, Uzxalqharakati.com, had already come under a distributed denial-of-service attack.

---


Uzbekistan

(DDoS) attack in January 2013, the third since its registration in May 2011. The attack paralyzed the website for several days.

The Uzbek authorities appear to have fairly sophisticated censorship technology at their disposal that enables them to not only block entire domains, but also restrict access to individual pages that contain politically sensitive content while retaining access to other parts of a particular site. For example, in February 2011, after people started discussing the protests that were erupting in the Middle East, including expressing solidarity with demonstrators and sharing news links about what was happening, users began reporting that certain pages and discussions on Facebook, LiveJournal, and Twitter were being blocked, though the social media platforms as a whole remained available. Similarly, in February 2012, the media reported that the Uzbek-language pages of Wikipedia were blocked, while their Russian counterparts remained available, although the latter typically contain more information on often-censored topics like human rights abuses. Analysts speculated that the block was more related to the government’s nationalistic wish to monopolize Uzbek-language content than because of concerns that users would access politically sensitive information.

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. There is a widespread suspicion of involvement from foreign firms providing networking equipment to Uztelecom for the purpose of state censorship over the internet. The architecture of Uztelecom’s network UzNet, which provides internet transit for private ISPs and internet access in governmental institutions, is based on network routers and switches produced by Cisco Systems, Inc. Moreover, in its daily operations, Uztelecom widely employs the equipment of the Chinese companies ZTE and Huawei. ZTE opened its Uzbek office in 2003 and became a leading supplier of USB modems, mobile phones, and routers to all mobile phone operators and Uztelecom. The government grants ISPs and mobile phone operators import duty and sales tax exemptions on the surveillance equipment that they are required to install on their networks at their own expense. However, the government reportedly abolished some of its import tax exemptions on telecommunications equipment in 2013.

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...”

---

67 Ozodlik.org, „Атака на сайт Народного Движения Узбекистана, [The attack on the website of the People’s Movement of Uzbekistan]“ January 27, 2013, http://www.ozodlik.org/content/article/24884770.html.
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.

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, which is integrated into the structure of the State Committee on CITT, 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 has contributed to the takedown of independent websites.

In August 2011, the government created a new secretive body—the Expert Commission on Information and Mass Communications—to oversee online controls, including the work of the Monitoring Center. The commission is not independent and must submit quarterly reports to the Cabinet of Ministers. Furthermore, its membership is not made public, although the body is reportedly comprised exclusively of government employees. The new commission is mandated to evaluate online publications and determine if they: (1) have a “destructive and negative informational-psychological influence on the public consciousness of citizens;” (2) fail to “maintain and ensure continuity of na-

---

74 According to government figures, only about 30 percent of websites with “.uz” domain names were hosted on servers based in Uzbekistan as of December 2011. See Uzinfocom, “Только цифры” [Only Numbers], January 5, 2012, http://bit.ly/1hbO2sN.
79 Resolution of the Cabinet of Ministers RU, “О дополнительных мерах по совершенствованию системы мониторинга в сфере массовых коммуникаций” [On Supplementary Measures for the Improvement of the Monitoring System for the Sphere of Mass Communications], No. 228, 5 August 2011, SZ RU (2011) No. 32-33, item 336.
80 Ibid., at Annex II, Art. 31.
81 Ibid., Annex I, containing a list of the Commission’s members, is not made public.
Uzbekistan

Tional and cultural traditions and heritage;” or (3) aim to “destabilize the public and political situation,” or commit other potential content violations.\(^{83}\)

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.\(^{84}\) 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.\(^{85}\) 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. As of February 2014, the Commission appeared to be functioning but little information on its activities is available. 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.\(^{86}\)

The speed at which authorities respond to controversial content online is evidenced in the case of UzMetronom.com, a popular Tashkent-based independent online newspaper launched in April 2006 and devoted to critical news reporting on Uzbekistan. On July 23, 2013, UzMetronom.com reported a fatal shooting between the Uzbek and Kyrgyz border patrol guards along the countries’ border. According to the news site’s founder, chief editor and independent journalist Sergei Ezhkov, UzMetronom.com reposted that information from the official news media site Podrobnno.uz.\(^{87}\) Despite the fact that UzMetronom.com is permanently blocked in Uzbekistan, one day after the information was posted, Ezhkov was called before the military prosecutor’s office in Tashkent. The editor received a “warning on the inadmissibility of the violation of law” and faced threats of criminal prosecution. According to the prosecutors, the news site had no right to publish details of the incident without obtaining “reliable information” from competent authorities. UzMetronom.com interrupted its reporting for three days.

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.\(^{88}\) 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.

\(^{83}\) Resolution of the Cabinet of Ministers RU, No. 228, at Art. 1 and Annex II, Art. 5. See note 50 above.

\(^{84}\) Ibid., at Art. 1 and Annex II, Art. 14.

\(^{85}\) Ibid., at Annex II, Arts. 26 and 29.


Uzbekistan

The editorial direction of the online versions of state-run news outlets is often determined by both official and unofficial guidelines from the government. For example, on orders of the president, a specific ideological theme dominated the news media landscape in 2013, dedicated to the implementation of the state policy program “2013 – The Year of Wellbeing and Prosperity.” The aim of the propaganda was to inform the public and “foreign specialists” on the current socio-economic reforms in Uzbekistan.\(^89\)

In an apparent effort to develop the country’s media and information society, President Karimov signed a decree in December 2011 that extends tax preferences to media outlets. Taking effect on January 1, 2012, the decree exempts media services from the value added tax (VAT) and decreases the single tax payment required of media organizations from 6 to 5 percent, among other changes.\(^90\) While the decree purportedly aims to strengthen “public control over the activities of state power and control,”\(^91\) observers have noted that without an overall change in the regime’s attitude to independent media, the new benefits are unlikely to have a meaningful effect on freedom of speech in the country.\(^92\)

Facebook, YouTube, Twitter, and the Russian social networks Odnoklassniki (odnoklassniki.ru) and VKontakte (vk.ru) continue to top the list of the most visited websites in Uzbekistan.\(^93\) In February 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 (@Gulnara-Karimova) to reveal inside secrets about her family and the corrupt practices of the Uzbek national security service.\(^94\)

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 a microblog Bamboo.uz, launched in February 2014 for the exclusive use by 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.\(^95\) 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 known clients of Skype and ICQ, Google Talk and Mail.ru.\(^96\) The service is available in Russian and Uzbek languages and can be used on mobile phones.

---

89 See Resolution of the President RU No. ПП-1920, note 11 above (cross-reference to check), at Annex (§ No. 83-86).
92 IREX, “Uzbekistan.”
Uzbekistan

In 2010, the state-run Uzinfocom Center began creating a “social media zone” specifically geared toward users of the ZiyoNet intranet in Uzbekistan. The zone includes a range of social media applications, including Id.uz (a social-networking site), Fikr.uz (a blog-hosting platform), Utube.uz (a video-sharing platform), Smsg.uz (an instant messenger service), and Desk.uz (a site for personal widgets). Access to these applications requires users to register either as an anonymous user or with their passport details. Although for the moment, the zone’s applications remain less popular than international brands, as of January 2014, over 70,000 people had registered at Id.uz. Uzinfocom Center’s close relationship to the government raises concerns over the pressure the applications may receive from the authorities to censor and monitor users.

Besides the social media zone aimed at ZiyoNet users, the social-networking website Muloqot.uz (meaning “dialogue”) was launched in September 2011 in an apparent effort to offset the growing influence of other popular social networks. It is open only to Uzbek citizens residing in Uzbekistan. On the first day the social network was launched, staff of the Uzbek service of RFE/RL reportedly registered accounts and posted RFE/RL content (which is blocked within the country) to a general “wall.” According to their reports, their profiles were deleted within 15 minutes. The servers of the website are located at the data center of the state-owned Uztelecom, implying that the authorities are able to conduct constant censorship.

The blogosphere in Uzbekistan is weak, largely of entertainment character, and, due to the repressive environment, unable to significantly facilitate public discourse on political and social issues. A handful of blogs critical of the regime are run by Uzbek dissidents (for example, Jahonnoma.com, Turonzamin.org, and Fromuz.com) or are affiliated with independent online news sites like Uznews.net or Fergananews.com. Since its establishment in January 2012, a forum at Choyxona.com 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.com, a forum site that was suspended in 2011 after Uzbek authorities arrested several of its users.

From December 5–8, 2013, the press center of a banned political opposition group in exile, the National Democratic Movement “Birdamlik” (birdamlik.info), used its website to mobilize for peaceful protests and distribute the text of the constitution of Uzbekistan in Tashkent. Three human rights defenders, Elena Uralaeva, Malakhot Eshankulova, and Shukhrat Rustamov, and 11 other participants of the protests in Tashkent were arrested. At the same time, social media tools have been important for exposing and disseminating information related to human rights abuses. In May 2005, for example, videos documenting Uzbek security forces opening fire on unarmed protesters in Andijan were uploaded to YouTube, and regular updates were posted on Arbuz.com, contributing to international condemnation of the incident.

98 Luke Allnutt, “Uzbekistan Launches Its Own Facebook, Except It’s Not For Everyone.”
Violations of User Rights

The environment for internet users’ rights in Uzbekistan is already one of the most restrictive in the region, with the government employing extensive surveillance measures to monitor online activity, as well as using trumped-up charges to target individuals who publish material online that is deemed counter to the government’s interests. In December 2013, one citizen was given an eight-year prison sentence for establishing communication over the internet with an Uzbek opposition group in exile and for distributing materials on the group’s orders that were perceived as violating the constitutional order. There were also several cases of arrest, intimidation, and prosecution of professional journalists. Since April 2014, online users face rigid surveillance at internet cafes due to new regulations.

The constitution of Uzbekistan guarantees the right to freedom of expression (Article 29) and freedom of the mass media (Article 62). It also prohibits censorship (Article 62). In practice, however, these constitutional rights are not fulfilled and are severely restricted by laws and government regulations. Judges lack the independence and impartiality needed to ensure the constitutional protection of speech.\textsuperscript{102}

The 1997 law “On Mass Media” was amended in 2007 with the purpose of altering the definition of “the press” to include “websites in generally accessible telecommunication networks.”\textsuperscript{103} This law neither defines nor establishes clear criteria for what constitutes a news-oriented website.\textsuperscript{104} In order to be regarded as part of the news media, websites are required to obtain an official registration certificate in a procedure similar to that required for traditional news media outlets.\textsuperscript{105} This procedure is generally known to be content-based and arbitrary, and inhibits editors and readers from exercising their freedom of expression.\textsuperscript{106} Applications for press certificates are supposed to include details such as the website’s digital media title, founder(s), language, aims and purposes, content specialization, domain name, sources of financing, editor(s), address of an editorial office, as well as affiliation of the founder(s) or editor(s) with other mass media outlets.\textsuperscript{107} Journalists or non-media professionals affiliated with registered online news media outlets are awarded certain rights and must abide by statutory conditions that are applicable to professional journalists, arguably creating, in practice, an

\begin{itemize}
\item[\textsuperscript{102}] Joint Resolution of the Plenums of the Supreme Court and Higher Economic Court RU “О судебной власти” [On the Judicial Branch of Power] No. 1, 20 Dec. 1996, as amended on December 22, 2006 (No. 14/151), at para. 3 (justifying the rule that all judges are appointed by the President of Uzbekistan).
\item[\textsuperscript{104}] Ibid.
\item[\textsuperscript{106}] UN Human Rights Committee, Mavlonov and Sa’di v. the Republic of Uzbekistan, Communication No. 1334/2004, Views adopted on April 29, 2009, UN Doc. CCPR/C/95/D/1334/2004, at paras. 2.6, 2.11 and 8.3.
\item[\textsuperscript{107}] Resolution of the Cabinet of Ministers RU No. 214, note 109 above, at Annex II.
\end{itemize}
environment where journalists’ key responsibility is “loyalty to the regime.” As of January 2014, 261 websites were registered as mass media in Uzbekistan.

The legislation regulating the exercise of freedom of expression applies equally to traditional news media outlets and the internet. Due to the 2007 amendments, the law “On the Mass Media” is applicable to overseas news media outlets whose content is accessible from within the territory of Uzbekistan, though no cases of this law being invoked by Uzbek courts against foreign websites have been reported so far. In addition, some laws have been used to punish individuals for posting or accessing content deemed to violate vague information security rules. Under the criminal code, slander (Article 139) and insult (Article 140)—including of the president (Article 158)—are criminal offenses that also apply to online content, as do provisions that punish activities such as “dissemination of materials posing a threat to public safety.” 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.

On September 10, 2013, Kudratbek Rasulov, a jeweler and resident of Namangan, was arrested at the request of the NSS and charged with threatening the constitutional order (Article 159 of the criminal code) and the production and dissemination of materials containing a threat to public security and order with foreign financial help (Article 244 of the criminal code). On December 27, he was sentenced by a city court to eight years in prison in a one-day trial. The judgment was based on an interpretation of records of communication that Rasulov established with the exile opposition group, National Movement of Uzbekistan (NDU), via Skype and the social networking sites, Odnoklassniki and Facebook. Rasulov was charged with receiving films and literature with extremist content from NDU and distributing several copies of a DVD titled “Freedom of An Unarmed Man” to strangers on the streets of Namangan. In its reasoning, the court also emphasized that Rasulov had been in contact with opposition leaders Mukhammad Salikh and Tulkin Karaev. His appeal was postponed by a court in January 2014 for an undetermined period of time, and as of May 2014, he was still in prison.

On September 21, 2013, Sergei Naumov, an independent journalist who has contributed reporting for the Ferghana News website and for the Institute for War and Peace Reporting (IWPR), was arrested and given a 12 day sentence on charges of hooliganism after he collided with a woman on the street. The woman complained to local police that Naumov had insulted and pushed her, which Naumov denies. Naumov is known for his reporting on human rights abuses, including reports on child labor conditions during the fall cotton harvest in Uzbekistan. After his arrest, IWPR issued a

---

statement expressing concern that Naumov’s detention was likely an effort to silence his critical reporting, a tactic the authorities are known for using against journalists in the country.115

It is also becoming increasingly difficult for professional photojournalists to work in Uzbekistan. On January 30, 2014, a swift trial took place for Umida Akhmedova, a women’s rights defender, documentary photographer and filmmaker,116 and her son Timur Karpov, a photo editor for the Russian news agency Lenta.ru. On January 27, 2014, they had participated in and took photos of a small picket protest outside the Ukrainian embassy in Tashkent involving a group of eight individuals who gathered in solidarity with Ukrainian protesters in Kyiv amid the country’s political crisis. All participants were arrested on January 29, interrogated throughout the night, and compelled to testify against themselves or plead guilty. They were charged with violation of Article 201 of the administrative code that regulates the organization and holding of meetings, rallies, marches or demonstrations. Timur Karpov was fined 5,766,300 Uzbek Sum (US$2,040) and Umida Akhmedova was fined 4,805,250 Uzbek Sum (US$1,700); both were released.117 The administrative case was tried in a criminal proceeding (in violation of Article 245 of the administrative code). The court also failed to provide the accused with adequate time and access to the defense council.

The authorities have also used legal proceedings and intimidation to shut down independent news sites in an already extremely limited media environment. For example, on January 19, 2013, Olam.uz, which at the time was Uzbekistan’s second most-visited news site, chose to go offline for “technical reasons,” according to its Facebook page. However, as independent sources report, the Uzbek authorities had opened up proceedings against its editor-in-chief and the website owner, the Tashkent-based LLC Mobile Mass Media.118 Charges included such offences as infringement of copyright and patent law, high treason, encroachment upon the constitutional order, espionage, subversive act, loss of documents containing state or military secrets, and robbery. At the time, Olam.uz was reporting extensively about the Uzdunrobita (MTS-Uzbekistan) case and allowing readers to leave comments on every article published.

As of May 2014, two Uzbek online journalists remained in jail, ostensibly on fabricated criminal charges.119 Solidzhon Abdurakhmanov, a reporter for the independent news website Uznews.net, continues to serve a 10-year sentence imposed in October 2008 for allegedly selling drugs. The 63-year-old journalist was not pardoned as part of the amnesty granted to all prisoners over the age of 60, which was enacted on the 21st anniversary of Constitution Day in December 2013.120 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 and

---

Uzbekistan

in retaliation for his reporting.121 Dilmurod Saiid, 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.122

The authorities have also used various forms of arbitrary detention and intimidation to silence online critics. In November 2011, the government released Jamshid Karimov, an independent journalist and nephew of the president, from a psychiatric hospital where he had been kept against his will since September 2006. Prior to his detention, he regularly published articles online, including about human rights abuses in Uzbekistan. He is widely believed to have been detained in retaliation for his journalistic activity. He suddenly disappeared again in January 2012.123

The use of proxy servers and anonymizers remains a very important tool and the only way to access content blocked in Uzbekistan. However, in September 2012, Uztelecom started a centralized and permanent blocking of proxy servers and websites enlisting free proxies without a web interface.124 At the same time, the use of both proxies and anonymizers require computer skills beyond the capacity of many ordinary users in Uzbekistan.

The space for anonymous online communication in Uzbekistan is steadily shrinking. In 2011 Arbuz.com, one of the country's most important online forums for anonymous discussion, was shut down after the arrest 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.125 According to some reports, the NSS had tracked them through their internet protocol (IP) addresses.126 Few options remain for posting anonymous comments on other online forums—such as Uforum.uz,127 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.128 Individuals must also provide a passport to buy a SIM card.129 There are no explicit limitations on encryption, though in practice, the government strictly regulates the use of such technologies.130

Although Article 27 of the constitution guarantees the privacy of “written communications and telephone conversations,” there is no data protection legislation in Uzbekistan. Officially 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.\(^{131}\) ISPs and mobile phone companies must install SORM and other surveillance equipment on their networks in order to obtain a license.\(^{132}\) 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.\(^{133}\)

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.\(^{134}\) If surveillance is part of a civil or criminal investigation, content intercepted on telecommunications networks is admissible as court evidence.\(^{135}\)

Since July 2004, operators of internet cafes and other public internet access places have been 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.\(^{136}\) Operators of internet cafes and public access places must install surveillance cameras on their premises as a new measure to “ensure 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 quite burdensome and expensive for internet cafe businesses in Uzbekistan.\(^{137}\)

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’


\(^{132}\) Ibid., at 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, at Arts. 208, 211, 230 part 2, and 269.

\(^{133}\) See Law RU, “On Telecommunications”.


\(^{136}\) 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-мх, SZRU (2014) NO. 13, item 150.

laptops, and interrogating individuals with a record of visiting websites critical of the government.\textsuperscript{138} Furthermore, on February 12, 2014, Marjam Ibragymova, a political scientist from Tashkent, was invited by prosecutors to 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.net and Fergananews.com under the pseudonym “Gulsara Vafaeva,” as well as views she expressed during an online talk-show “Шут ме” (Uznews.net). She was compelled to sign a statement on “inadmissibility of such actions in the future.”\textsuperscript{139}

There were numerous instances of technical attacks against news websites in Uzbekistan during 2013-2014. In November 2013, the websites of four independent and one state-run mass media outlets fell victim to distributed denial-of-service (DDoS) attacks. On November 14, massive DDoS attacks (1Gbps) were launched against three independent news sites: CA-News (Centrasia.ru), Fergananews.com, and UzMentronom.com.\textsuperscript{140} Presumably launched from IP addresses located in Russia and Kyrgyzstan, among other places, these attacks paralyzed the websites for several days. This DDoS attack seemed to have had a connection with the massive DDoS attack against the international broadcaster Radio Free Europe/Radio Liberty and the Uzbek service at Ozodlik.org, on November 18.\textsuperscript{141} On November 19, the hacker group known as BD Grey Hat Hackers defaced the state-run Xalq So‘zi newspaper’s websites in Uzbek (xs.uz) and Russian (Narodnoeslovo.uz).\textsuperscript{142} It is not clear whether the same hacker group is responsible for the DDoS attacks on the independent news sites. On March 17, 2014, the news site UzMetronom.com again reported hacker attacks on its website.

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.\textsuperscript{143} The Centre took over the functions and competences of the Uzbekistan Computer Emergency Readiness Team (UZ-CERT), established in 2005.\textsuperscript{144} In particular, the Centre continues to alert internet users on 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 enforce-
Uzbekistan

ment—on the prevention and investigation of “unsanctioned or destructive actions in information space.”145

Venezuela

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>53</td>
<td>56</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 29.7 million

- Internet Penetration 2013: 55 percent
- Social Media/ICT Apps Blocked: Yes
- Political/Social Content Blocked: Yes
- Bloggers/ICT Users Arrested: Yes
- Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- Amid a government crackdown on protests in February 2014, internet service was down for approximately 36 hours in San Cristobal. Additional service disruptions were reported throughout the country (see Obstacles to Access).

- In late 2013 and early 2014, the Venezuelan government blocked nearly 400 websites providing information on politics and economic issues, such as currency exchange rates and political demonstrations (see Limits on Content).

- In February 2014, CONATEL blocked the website of NTN24, a Colombian news group, after it aired video of a protester being killed; the regulator also blocked images of the protests on Twitter and blocked apps facilitating organization, such as Zello and Tunnel Bear (see Limits on Content).

- In June 2013, a Venezuelan court made its first official ruling specifically forbidding an individual from using social media (see Violations of User Rights).
Introduction

In a country where all government branches act in compliance with the interests of the ruling party, ensuring a hegemonic media landscape, the Venezuelan people widely use the internet to participate in forums that allow independent expression, particularly social networks. As a result of the government’s ongoing siege against private media—which includes the takeover of newspapers by progovernment owners—traditional media outlets have ventured into the digital arena. Due to the comparatively low barriers to entry, new businesses have appeared in this environment as well. It is in this atmosphere that Twitter, Facebook, YouTube and similar platforms have become the final refuge for independent voices and freedom of expression.

Since Nicolás Maduro was elected president following the death of Hugo Chávez in March 2013, the Venezuelan currency has been devalued multiple times, and inflation has risen to 56 percent—the highest rate on the planet. Venezuela’s capital has one of the highest murder rates in the world, and shortages of basic food items and toiletries have become part of daily life for millions of Venezuelans. Due to these crises, protests are increasing, as are government efforts to influence online discussions and to restrict online content. In response to the threat of growing online activism, Minister of Communication and Information Delcy Rodríguez has identified social networks as a breeding ground for “perpetrators of coup-leading violence” and others seeking to “cause large-scale psychological distress in the population.” In a move that is rather unsurprising given its distrust of social media, the Maduro administration recently created a regulatory body known as the Vice Ministry of Social Networks specifically focused on this new arena.

The state has long held near complete control of the digital environment through Venezuela’s main internet service provider (ISP), the National Telephone Company of Venezuela (CANTV), and through the communications regulator, the National Telecommunications Commission of Venezuela (CONATEL). In recent years, however, citizens have persevered in creating online forums for propaganda-free news, social activism, and the voicing of critical opinions. In response, the

5 In 2013-2014, the largest devaluation in Venezuela’s history took place. According to the different exchange rates, it represents a devaluation between 358 and 722 percent. See: Miguel Angel Santos, “Lunes Negro y Los Huecos del Ajuste Rojo,” [Black Monday and the Holes of the Red Cut], El Universal, March 26, 2014, http://goo.gl/lMcKt2
government has increased efforts to block the circulation of political and economic content through the web—as well as at times restricting internet access itself—initiatives that have slowed the growth of internet penetration rates and connection speeds.

By mid-2014, CONATEL had ordered the blocking of some four hundred sites and portals containing economic and political information. It is worth noting that such blockings were carried out as discretionary measures, executed without legal procedure. Private ISPs complied with government orders on blocking out of fear of the severe sanctions threatened by CONATEL for those providers that allowed the circulation of such content.\(^1^0\) In February 2014, following widespread protests over violence, insecurity, shortages of basic goods, and an increasingly hostile political environment, connection to the broadband service provided by CANTV (which accounts for the majority of internet subscriptions) was unavailable for over 36 hours in San Cristóbal. The website that hosts Twitter images, as well as the apps Zello and Tunnel Bear, were each sporadically blocked; foreign news media was barred; and the cellphones of those recording government abuses were confiscated.

By the time the protests, which lasted from February to June, had ceased, thousands had been arrested on political grounds, hundreds had been injured, and over forty had been killed. Allegations of state brutality ran rampant, and international organizations, such as the United Nations and Human Rights Watch,\(^1^1\) decried the Venezuelan government's infringement on freedom of expression, both online and off, as well as its treatment of its own people. The hacking of political websites and the usurpation of the Twitter profiles of political activists, critical journalists, and dissident voices—a damaging trend which began in 2012— also continued to plague Venezuelans, as did harassment targeting opposition members and those critical of the ruling party.

**Obstacles to Access**

The internet arrived in Venezuela in 1992, with CONATEL granting licences to the first ISPs in 1996.\(^1^2\) While the 1999 constitution obligates the state to provide the public with access to new information and communication technologies (ICTs),\(^1^3\) the Organic Law of Telecommunications, which was reformed in December 2010, declares ICTs an area of state interest, prioritizing government use over public access to ICTs.\(^1^4\) In several recent cross-country studies assessing ICT trends over the past

---


Venezuela

five years, Venezuela is among the countries that have fallen farthest in the rankings relative to its peers, such as Colombia and Ecuador, whose internet environments have been improving.\textsuperscript{15}

The Venezuelan government hopes to expand and improve internet access via the National Transportation Network,\textsuperscript{16} through which it will install nearly 7,000 kilometers of fiber-optic cable.\textsuperscript{17} Official sources indicate that between 40 and 60 percent of the works commissioned by CANTV have been concluded,\textsuperscript{18} but the projects are reportedly behind schedule and no independent firm has yet conducted an audit.\textsuperscript{19} The government is also hoping to increase computer literacy through its CANAIMA project, which aims to bring computers to classrooms throughout the country. According to official figures, over three million laptop computers\textsuperscript{20} have been given to Venezuelan elementary school students to this end. However, while not all computers are equipped with internet connectivity, they are equipped with proselytizing educational materials that glorify the administration\textsuperscript{21} In April 2014, CONATEL announced a new National Telecommunications, Information Technology, and Postal Services Plan, which promises an internet penetration rate of 100 percent by 2020. While it seems doubtful that Venezuela will be able to increase penetration from 55 percent to 100 percent in six years, it will be interesting to follow the progress of the Plan, which also contains strategies to develop political content supporting revolutionary democracy and socialist ethics.\textsuperscript{22}

The latest data from the International Telecommunications Union (ITU) reveals that internet penetration in Venezuela increased by approximately six percent between 2012 and 2013, rising to 55 percent by year’s end.\textsuperscript{23} According to data provided by the consultancy firm ComScore, Venezuelan internet users are predominantly young and urban, with 72 percent falling between 15 and 34 years of age.\textsuperscript{24} Venezuela is home to nearly 12 million Facebook users and over 3 million

\begin{thebibliography}{999}
\bibitem{17}The National Transportation Network should connect the Orinoco-Apure region (the southern half of the country) with the northern coastal region, with 213 nodes distributed in 18 states. The states the network goes through are: Amazonas, Anzoátegui, Apure, Arauca, Barinas, Bolívar, Cojedes, Falcón, Guárico, Lara, Mérida, Miranda, Monagas, Portuguesa, Sucre, Táchira, Trujillo and Zulia. See: CONATEL, “Conatel Abandera Inclusion Social con la Red Nacional de Transporte,” [Conatel Championed Social Inclusion with the National Transport Network], January 31, 2014, \url{http://gqo.qi/ppj1GV}.
\bibitem{18}Medios Comunitarios (website), “Conatel Abandera la Inclusión Social con la Puesta en Marcha de la Red Nacional de Transporte, [Conatel Champions Social Inclusion with the Launch of the National Transport Network], October 18, 2013, \url{http://gqo.qi/sfReS}.
\bibitem{20}Ultimas Noticias, “Gobierno Venezolano Ha Entregado 3,3 Millones de Canaimas,” [The Venezuelan Government Has Delivered 3.3 Million As Part of Canaima], November 8, 2013, \url{http://gqo.qi/T79zq}.\bibitem{21}The program started in 2009 and aims to provide computers to children in elementary schools. In 2014, high school students were incorporated into the program. This strategy has been questioned because it includes software containing government propaganda. For more, see: \url{http://www.canaimaeducativo.gob.ve/}; See also: Fidel Salguero, “Acumuladores Duncan: Una Historia para Tenerla Presente,” [Acumuladores Duncan: A Story to Keep in Mind], Inside Telecom, Vol. XIV, #45, November 28, 2013.
\bibitem{24}ComScore, “Futuro Digital Venezuela 2013,” [Venezuela Digital Future 2013], December 9, 2013, \url{http://gqo.qi/kjfc8}.
\end{thebibliography}
Twitter users. Key topics disseminated and debated through these mediums include politics and news, and, increasingly, concern over shortages of basic goods and rising inflation.

According to CONATEL’s latest statistics, 61 percent of internet subscriptions are fixed household connections and 32 percent are wired connections. The remainder are classified as “non-residential,” but it is not clear if this refers to mobile phone subscriptions or business accounts. While more people are now connected to the internet, the majority of the population has access only to narrowband service. Although the average regional speed of internet connection for Latin America is 2.5 Mbps, according to the latest report from Akamai, Venezuela has an average of only 1.27 Mbps. For comparison, Bolivia, which is much less developed, ranks last, with a speed of .95 Mbps. Nationally, state-owned CANTV—which holds over 80 percent of internet subscriptions in Venezuela—offers prepaid plans with minimum connection speeds of 1 Mbps at a cost of about US$10.50 per month, or 1.5 Mbps at a cost of US$22.81 per month, as compared to a minimum wage of approximately US$519 per month. In late 2013, a 6 Mbps plan was announced at a cost of US$95.23. The fee for this plan, however, represents a significant portion of the minimum wage and is only available in select areas. The second most widely used ISP, Inter, offers a connection speed of 10 Mbps for US$88.25—seven dollars less for a connection that is 66 percent faster.

In addition to poor quality and low internet speeds, geographic isolation in rural areas, low computer literacy, and the expense of necessary equipment also pose substantial obstacles to access. The regional divide in internet access in Venezuela is noteworthy; while in the Capital District and the State of Miranda the percentage of individuals with internet access exceeds 90 percent, in states such as Amazonas, Yaracuy, and Apure, penetration hovers around 15 percent. Connectivity in rural areas has been further compromised by a severe electricity crisis that has led to rationing in every city but the capital. Regional disparities are also evident in the expansion plans.

---


28 Agencia Venezolana de Noticias, “En Cuatro Años CANTV Pasó de 0, 7 a 1, 5 Mbps de Velocidad en Internet,” [In Four Years CANTV Went from 0.7 Kbps to 1.5 Mbps in Internet Speed], May 3, 2014, http://goo.gl/TEKQoX.


30 This figure is based on a personal analysis that takes into account sources such as CONATEL and the ITU, as well as interviews with experts and representatives of national telecommunications companies who prefer to remain anonymous.


33 The services of Inter are offered only in major cities. The 10 Mb plan has been offered since April 2011. At first it had a limit of 25Gb of consumption, but it was later turned into an unlimited consumption plan.

of telecommunications companies, which typically focus new investments on the most economically vibrant cities and surrounding areas.\(^\text{35}\) By the end of 2013, mobile phone penetration in Venezuela reached 101.6 percent.\(^\text{36}\) This figure does not necessarily reflect a population saturated with mobile technology, however; some Venezuelans have as many as three phones, each of which is associated with a different mobile provider, in order to ensure countrywide coverage. Over one third of Venezuela’s mobile subscriptions utilize CDMA technology. Digitel began offering 4G LTE services at the end of 2013, but only to limited cities.\(^\text{37}\) While there are approximately 30 telecommunications operators in Venezuela, only three provide mobile phone services. Movistar, the Venezuelan unit of Spain’s Telefónica, has nearly 11 million subscribers; Digitel, a locally owned private company, has approximately 5 million subscribers; and CANTV’s Movilnet, which leads the market, has 16 million subscribers out of a total of 32 million.\(^\text{38}\)

As of 2014, mobile internet penetration in Venezuela was measured at seven percent.\(^\text{39}\) Venezuela ranks fourth in Latin America in terms of connection speeds via smartphone, with connections surpassing 1.5 Mbps only in a few zones.\(^\text{40}\) Those who do have smartphones typically live in urban areas and have higher than average income levels. Although the number of users with smartphones and data plans is growing, currency exchange controls and the devaluation of the Venezuelan bolivar have resulted in high prices and limited supplies.\(^\text{41}\) The networks run by private mobile service providers suffer from severe congestion and require further development, yet discriminatory currency controls have forced providers to ration their services and decrease investment in infrastructure.\(^\text{42}\) An industry executive who chose to remain anonymous for fear of governmental reprisals stated that during 2013, the private sector received 50 percent less foreign exchange assignment than state enterprises, evidence of biased funding.\(^\text{43}\)

Further complicating matters, the CANTV initiative, “Buy Made in Venezuela,” which aims to give preference to locally produced cell phones manufactured by Vtelca and Orinoquia in partnership with the Chinese firms ZTE and Huawei, has not satisfied demand, and the state’s blocking of


\(^{41}\) Producto Magazine, “Movistar y Digital Sin Inventario,” [Movistar and Digitel without Inventory], January 24, 2013 http://goo.gl/A8knk2; accessed April 15, 2014


\(^{43}\) Inside Telecom, Vol XV No. 4, January 30, 2014.
foreign currency has made it difficult to import mobile phones from foreign manufacturers. 44 These two factors have resulted in a shortage of cell phones within the country which has led to price speculation (in this case, the artificial inflation of the cost of mobile phones) and which has weakened the sustainability of mobile phone businesses. 45 As of the second quarter of 2014, the inventories of mobile phone operators were practically empty. 46

In a disturbing trend, substantial interruptions of telecommunication services have begun to occur. 47 During the highly contested April 2013 presidential election, CANTV shut down broadband service for approximately 30 minutes, leaving 95 percent of Venezuelans disconnected from the internet at a crucial time. In September 2013, reported damage to a section of fiber-optic cable left three regions without internet service. 48 In the November 2013 lead-up to municipal elections, CANTV’s broadband internet service was down for approximately two hours. 49 Disruptions were reported in Caracas, Maracaibo, and Mérida, among other cities. As in previous instances, authorities offered no explanation for the service disruptions, all of which occurred at critical times.

The latest—and longest—service interruption occurred in San Cristóbal in mid-February 2014 during nationwide protests. CANTV’s internet service was unavailable for 36 hours in the city, as well as in other parts of Táchira state. Although the government denied responsibility, alleging that the blackout was due to vandalism or fire damage, the disruption occurred during an announcement from the Minister of Defense about measures to control political demonstrations in San Cristóbal, which had been underway for approximately 15 days at that point. 50 Such restrictions on ICT connectivity during pivotal times is a continuing concern in Venezuela. Service disruptions and rumors of internet throttling—the intentional slowing down of service to effectively cripple online activity—were also common during the 2014 protests. 51 Applications such as the walkie-talkie program Zello (which the Minister of Communication and Information claimed was a platform for the promotion of terrorist activity) 52 and Tunnel Bear VPN Service, 53 often used by protesters as a
Venezuela

means of communication and to bypass censorship, were both blocked by the government during protests. The director of technology for Zello, who believes that the Venezuelan government was behind the block, responded actively, adapting the app with a changing IP address that makes it more challenging to obstruct.54

While there are no special restrictions on the opening of cybercafes in Venezuela, their numbers have been declining because of a marked drop in interest among youth. Observers suspect the decline is the result of government restrictions on the types of games that can be installed on computers at cybercafes. Among its restrictions, the 2009 Videogame Law,55 which has only recently been enforced, prohibits the installation of “war related games” and bans students in school uniforms from entering cybercafes unless accompanied by a teacher.56

Although privately owned ISPs do exist, the state monopolizes the internet market through CANTV, a factor that allows for greater government control of internet services. Following its 2007 renationalization, a move that benefited CANTV significantly in regard to currency controls,57 an improvement in service was expected, but, to date, quality remains poor. All earnings obtained by the company are reserved for social programs rather than being reinvested to improve ICT offerings.58 Despite CANTV’s poor service record and slow connection speeds, its relatively low prices allow the company to remain dominant.59 Private providers have had difficulty competing with CANTV’s rates,60 and the lack of competition has reduced incentives for providers to retain high quality service or to expand their offerings.61 Investment in and expansion of the private ICT sector are further complicated by an economic environment characterized by very strict and politically discriminatory foreign currency exchange controls that make it difficult for private companies to access foreign currency in order to invest, maintain infrastructure, and repatriate their earnings.62 For

---

56 The “Video games” Law was passed in 2009 and can be accessed here: http://www.scribd.com/doc/83657622/Ley-para-la-Prohibicion-de-Videojuegos-Belicos-y-Juguetes-Belicos-3-de-marzo-del-2009. From the sanctions in Article 13: “Whoever promotes by any means the purchase or use of war related videogames or toys defined in this law will be sanctioned with a fine of two thousand to four thousand tributary units.” Article14: “Whoever imports, produces, sells, rents, or distributes war-related videogames, or military toys, will be sanctioned with prison from three to five years. The penalty provided in this article, and imposed by a final verdict, entails the seizure and destruction of the war-related videogames and war toys.”
60 Inside Telecom, Volume 7 No. 86 (2011): In late 2012, after 14 months of request, Movistar was given the authority to increase its rates from 9-17 percent for annual inflation. Movilnet, for its part, increased 32.6 percent (excerpt from newsletter; not available online).
small enterprises and individuals, exchange controls have also complicated the process of paying hosting providers, acquiring electronic devices, and conducting online shopping.63

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. 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 Directive Council. 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.64

In addition to making oversight nearly impossible, these arbitrary shifts in control are evidence of CONATEL’s lack of independence from the executive. The state also controls CENCOEX (the body formerly known as CADIVI). CENCOEX is the body responsible for unilateral control of the allocation and repatriation of foreign exchange, which is required by private telecommunications companies to improve and maintain their infrastructure. Given the near total control of the ICT sector by the government and its proclivity to exercise bias and avoid rule of law, any independent oversight of these bodies is impossible.

Limits on Content

In late 2013 and early 2014, the Venezuelan government blocked nearly 400 websites providing information on politics and economic issues, such as currency exchange rates and political demonstrations. In February 2014, CONATEL blocked the website of NTN24, a Colombian news group, after it aired video of a protester being killed; the regulator also blocked images of the protests on Twitter.

Venezuelans are avid users of digital media, which has emerged as an important platform for circulating information and expressing opinions at a time when independent television and radio stations have come under increased pressure.65 Over the past few years, however, the state has begun turning its attention to the internet as well. In December 2010, the National Assembly adopted a reform of the 2004 Law of Social Responsibility in Radio and Television (the ResorteME Law), extending regulation to online and electronic media. Under this law, online media outlets must establish mechanisms to restrict content that violates the law; however, matters are complicated by vague descriptions of prohibited content. Article 27, for example, forbids messages that promote anxiety among the population or alter public order, that disregard legal authorities, or that promote the violation of existing laws. Websites found in violation may be fined up to VEF 25,000

---

63 Small entrepreneurs use credit cards to pay for services or make purchases. The amount of foreign exchange they are allowed to use has been reduced from $3000 to $300 per year. See: Luis Carlos Díaz, “Venezuela: Compras por Internet Están Bloqueadas Desde Inicios de 2014,” [Venezuela: Internet Purchases Blocked Since Early 2014], CNET (Website), January 23, 2014, http://goo.gl/xk2qUY


65 Antonio María Delgado, “Venezolanos Burlan el Acoso a la Prensa de Maduro Gracias a Internet,” [Venezuelans Outsmart Maduro’s Harassment of the Press Thanks to the Internet], El Nuevo Herald, December 4, 2013 http://goo.gl/V8mKs
CONATEL has demonstrated a progovernment bias since it began to make administrative decisions under the banner of the ResorteME Law, such as blocking websites without judicial process and threatening to hold ISPs who object legally responsible.  

Venezuela has a history of placing restrictions on websites containing important social and political information, yet decisions to block content are neither transparent nor accompanied by an appeals process. In a move uncharacteristic of state regulatory bodies, the government did make an open announcement in November 2013 detailing CONATEL’s blocking of websites that informed citizens of the price of the so-called “parallel dollar;” however, the block—which has been in place for over six months—has now extended to nearly all sources of economic information.

CONATEL also urged the e-commerce portals Tucarro.com and Tuinmueble.com not to publish prices of vehicles and real estate. Both sites were threatened with closure for their alleged role in what the government is calling an “economic war” against the president. CONATEL further claimed that the sites were in violation of Article 27 of the ResortME Law and threatened to hold ISPs responsible as intermediaries, making them legally liable for hosted content. The regulator also requested that Twitter block accounts linked to websites that show prices of foreign exchange differing from Venezuela’s official rates; however, Twitter refused the request. 

The domain .co and others such as popular link shortener bit.ly were also temporarily blocked, reportedly to prevent Venezuelans from accessing an audio file, circulated primarily on Twitter, that featured the voice of deceased President Hugo Chávez, for fear that it might cause unrest.

Pro-opposition and independent news websites have also been blocked or disabled at various times, along with the website of the country’s National Electoral Council, which was temporarily unavailable.

---


69 The “parallel dollar” is the black market rate, which is 12 times more expensive than the official dollar. A foreign currency exchange control has been in place in Venezuela since 2003 and, progressively, the distance between the official exchange rate and the black market dollar price has been widening. Currently, this rate is about 10-12 times higher than the official one. For more, see: John Otis, “Venezuela Tries to Suppress Reports of Economic Upheaval,” Committee to Protect Journalists (Blog) December 3, 2013, http://goo.gl/im3z20

70 SIBCI, “Conatel Efectúa Reuniones Para Aplicar Regulaciones a Sitios Web Que Ofertan Bienes,” [Conatel Makes Meetings to Implement Regulations to Websites that Offer Goods], November 9, 2013, http://goo.gl/2lnukw

71 John Otis, “Venezuela Forces ISPs to Police Internet,” Committee to Protect Journalists, December 12, 2013 http://goo.gl/Q1jicm

72 Noticias 24, “Conatel Solicita a Twitter Bloquear Cuentas Vinculadas con Webs Que Ilicitamente Cotizaban Divisas” [Conatel Asks Twitter to Block Accounts Linked to Websites That Illegally Quote Currencies], November 19, 2013, http://goo.gl/7colPS


Venezuela

from both inside and outside of the country at key political moments.75 Despite the availability of human rights websites such as Freedom House, Reporters Without Borders, and Amnesty International, and the growing popularity of social media networks,76 websites such as Diariodecuba.com, Analisis24.com, and even Anonymouse.org—an anonymous proxy service—remain inaccessible to Venezuelans who access the internet via CANTV. Sites like Infodio.com, dedicated to revealing corruption among high government officials, have been blocked by CANTV as well as by private ISPs.77 Between February and May 2014, some 184 websites were inaccessible to CANTV internet subscribers.78 Freedom of information activists José Luis Rivas, Andrés Azpúrua, and Oliver Rivas have further suggested that private ISPs blocked additional sites at the behest of the government.79

Venezuela has more than three million registered Twitter users, occupying thirteenth place in the world and the fourth place in Latin America.80 Media with high circulation, such as the newspaper El Universal, have also started to circulate via the internet, which has become a forum for voices not supported in traditional, state-run media.81 Due to exclusion from public channels and reduced space in private media during the 2013 presidential campaign, opposition candidate Henrique Capriles launched his own channel on the internet, Capriles.tv.82 Although Capriles.tv is seen by few people due to lack of necessary bandwidth, Capriles has also made active use of Twitter to connect with his supporters, and has now surpassed the four million followers claimed by late President Hugo Chavez.83

As use of social media has flourished, online campaigns in support of political figures and basic civil rights have become ubiquitous, and social media has become the last space in which Venezuelans do not practice self-censorship. A message from Capriles, which translates as “Venezuela, to take care of you I have only this, my life,” became the most retweeted message in Venezuela to date.84 Celebrities joined in, using the hash tag #yosoyvenezolano (#iamvenezuelan), which at one point ranked first in Twitter’s worldwide trending topics, to show their support for Capriles.85 After the presidential elections, cyber activists joined forces through the website of human rights NGO Provea to dismantle fake news spread by the government in which the opposition was blamed for setting

---

84 Quote taken from Henrique Capriles’ Twitter page, April 5, 2013, https://twitter.com/hcapriles/status/320241677115731968
Venezuela

fire to several medical centers staffed by Cuban personnel—fires which, it turns out, never occurred.\textsuperscript{87}

A number of other initiatives, like the Twitter account @ustedabuso (you were abused), were created to allow citizens to report on violations of electoral law and to mobilize support for candidates. During the election, the so-called #Operacionavalancha, which sought to mobilize opposition voters, became a trending topic and garnered, on average, more than 120 messages per minute with thousands of retweets. Not all online campaigns have been as successful, however. In March 2014, a movement aimed at drawing international attention to the protests spread under the hashtag #OscarsForVenezuela, asking celebrities to mention the repression in their acceptance speeches. In response to the popularity of the campaign, Venezuelan authorities banned the airing of the awards show within the country for the first time in 39 years.\textsuperscript{88}

Manipulation of online content by the ruling party and its supporters has compromised the atmosphere of free online debate of sociopolitical issues, and has further suggested systematic controls on content.\textsuperscript{89} CONATEL has urged the media to avoid using the word “looting” in reports on citizens’ responses to shortages of food and basic supplies.\textsuperscript{90} In response, journalists from TV channels Venevisión and Globovisión opened Twitter accounts in order to inform their followers about the pressure they were under from the government and station owners alike to censor themselves.\textsuperscript{91} In May 2013, Google’s transparency report included a request for removal of content from a Venezuelan state agency for the first time.\textsuperscript{92} Although the specifics were not published, it is assumed that the content in question was related to one highly publicized case, in which the Venezuelan government accused Google of ridiculing President Nicolás Maduro by allowing a distorted image of the President to appear in search results.\textsuperscript{93} Google appears to have responded to the request in a manner which satisfied the Venezuelan government, although the details are unclear.\textsuperscript{94}

The government is also making substantial use of social media platforms to propagate its point of view and counter political opposition. The Socialist Party of Venezuela (PSUV) proactively disseminates its views and counters opponents through progovernment platforms, such as the website Apporrea.org, launched in 2002, and the Twitter feed @RedVergataria, launched in 2011 with the support of CANTV’s Movilnet and the Ministry of Popular Power for Science and

\textsuperscript{87} Provea (Website), \url{http://www.derechos.org.ve/}; See also: Rafael Uzcátegui, “Provea y la Quema de Los CDI,” [Provea and the CDI burning], April 22, 2013, \url{http://goo.gl/Fzyqvq}

\textsuperscript{88} Brian Ries, “Venezuelan Protesters Ask Oscar Winners to Speak Up,” Mashable, Mar 2, 2014, \url{http://goo.gl/m8itNH}


\textsuperscript{90} Alfredo Meza, “ ‘Saqueo,’ Esa Palabra Proscrita,” [‘Looting,’ That Banned Word], \textit{El País}, November 14, 2013, \url{http://goo.gl/6Pmu1}

\textsuperscript{91} For example, @VVperiodistas and @GVSinCensura from TV Channels Globovisión and Venevisión


\textsuperscript{93} Europa Press, “Venezuela Acusa a Google de Ridiculizar a Nicolás Maduro con una Imagen Distorsionada,” [Google Accused of Ridiculing Nicolas Maduro with a Distorted Picture], May 17, 2013, \url{http://goo.gl/oldLukt}

\textsuperscript{94} Últimas Noticias, “Google Retira la Imagen que Distorsionaba el Rostro de Maduro,” [Google Removes the Image that Distorted Maduro’s Face], May 17, 2013, \url{http://goo.gl/o2Pmxf}
Technology. President Nicolás Maduro has also urged his followers to fight opponents through social networks and via a “virtual army” known by the acronym TROPA (Revolutionary Tweeters Organized for the Homeland) whose mission is to disseminate government propaganda and catapult anti-opposition messages to the top of Twitter’s trending topics.

In recent years, the government has begun to blame unrest on social media. In May 2013, after the highly contested presidential election, National Assembly deputy Pedro Carreño blamed ensuing violence on posts published on Twitter, and subsequently announced a bill to regulate social networks. In December, the same deputy announced that the ruling party (which has the parliamentary majority) would promote the enactment of a “unique communication law” and that the ResorteME Law would be reformed again.

Continuing its trend of shifting focus to social media, the government recently created a body known as the Vice Ministry of Social Networks, which is focused solely on observing, regulating, and utilizing this new medium. In March 2014, the government created a database known as “Troop of Joy and Peace,” to face what it calls the “Twitter War.” Chavista militants can register to “defend the revolution” through the portal Tuiteros.org.ve. The government has also published governing regulations for a new body known as the Strategic Center for Security and Protection of the Country (CESPPA) created in autumn 2013 to monitor the internet for content that might affect “state policies.” CESPPA's specific response plan for such content remains unclear, but the vague language used in the new regulation appears to give it great discretionary authority.

Between February and March 2014, petitions were launched by the Venezuela chapter of the Internet Society (ISoc), the Acceso Libre initiative, and a group of free software activists.

---

100 Últimas Noticias, “Crean Portal Web Para Tuiteros Chavistas,” [Government Launches a Website for Chavistas Twitter Users], March 18, 2014, http://goo.gl/v0c52R; The first Venezuelan “Twitter Users for Peace” meeting was also recently hosted at the headquarters of state-owned CANTV, where the president announced that the government was planning to organize a regional, Latin American meeting, of “Tweeters for Peace.” See: Samantha Badgen, “Venezuelan President Calls for Latin American Summit of Chavista Twitter Users,” Journalism in the Americas, March 20, 2014, http://goo.gl/KsjBGZ
advocating for freedom on the internet and the end of internet censorship in Venezuela. During a late April teleconference in Estonia, U.S. Secretary of State John Kerry also publicly asserted that the Venezuelan government had restricted freedom of expression online, impeding internet access and blocking websites in order to counter what he called peaceful antigovernment protests.106

Despite the state’s growing barriers to diversity of opinions online, in May 2014, the NGO Instituto Prensa y Sociedad (IPYS) launched a collaborative platform known as Poderopedia, which, with the use of data visualizations, provides an unbiased “who’s who” in business and politics.107 Renowned freedom of information activists, such as Luis Carlos Díaz and Naibet Soto, have also recently launched live feeds on YouTube where they discuss political issues; both of these channels have become very popular among young Twitter users, and, as yet, remain unhampered by any state monitoring.108

Although social media has rarely been used to mobilize people in the past, on February 11, 2014, local opposition leaders, students, and journalists alike began to turn to social media to organize protests. Hundreds of journalists turned out for a rally, spreading the word on Twitter under the hashtag #MarchaPorLaPrensa (March for the Press). Twenty-four hours later, on National Youth Day, nascent popular demonstrations were bolstered by thousands of students voicing their frustration with the country’s growing economic insecurity. Around the same time, Leopoldo López, the leader of the small but emerging political party Voluntad Popular (Popular Will), called on his supporters to take to the streets to protest worsening conditions, using the hashtag #LaSalida to get the word out.

In response to the protests, the administration greatly intensified its crackdown on both traditional and new media. After graphic images of injured protesters appeared on Twitter under the hashtags #12F and #SOSVenezuela, Venezuelan ISPs blocked Pbs.twimg.com, the site that hosts Twitter images, rendering photos inaccessible within the country. A separate block prevented Venezuelans from reaching the text-hosting site Pastebin.109 No official explanation was provided for the loss of access to these general-purpose communications platforms; however, Nu Wexler, a spokesperson for Twitter, affirmed that the government was behind the blocking.110 Twitter also posted a tweet explaining how to use the service through SMS in case of restrictions on access to the site.111 Although many government supporters denied any CONATEL responsibility, a government representative later allowed that “some blocking” was necessary to combat online attacks and acknowledged having blocked 384 sites.112

109 José Luis Rivas, “Yes, We Were Censored. Proof of the Block on Twitter Images and Pastebin in Venezuela,” blog of José Luis Rivas, accessed on April 30, 2014; See also: Pastebin Account, https://twitter.com/pastebin/status/435879980707225600
The Maduro administration also revoked (and soon restored, presumably due to international pressure) the credentials of CNN reporters, pressuring them to leave through threats and harassment. The government then banned coverage of the protests by all nonstate outlets, removing Colombia-based news channel NTN24 from Venezuelan cable services and blocking its website after it aired footage of a student who was shot and killed during the protest. The Twitter account of the news channel NTN24 was also hacked.

During the protests, Juan Comerma, vice president of technological infrastructure for Movistar, stated that data consumption rose by more than 35 percent, primarily due to images and YouTube videos linked from platforms such as Twitter. While most of the protest images that were uploaded were legitimate, a handful of social media users began posting forged images from unrest in Egypt or the Palestinian territories, and claiming that they were photos of the violence underway in Venezuela. Although small, this campaign of disinformation provided the government with the evidence it needed to call into question all of the protest photos that had been shared on social networks. At the same time, the government made use of a similar technique as part of a ruse to present evidence that news of the protests had been exaggerated.

Despite the dual campaigns of disinformation, the true scope of the unrest and the police response were eventually disseminated online. During the demonstrations, online activists and citizen reporters recorded serious attacks on human rights by security agencies such as the Bolivarian National Intelligence Service (SEBIN) and the National Guard and disseminated them via YouTube and Twitter. Professional journalists then used these sources to assemble coverage that made the repression evident and forced the government to arrest those responsible, many of whom were members of the police and other bodies of state security.

### Violations of User Rights

In Venezuela, there are many avenues by which bloggers, journalists, and private citizens can be punished for content posted online. The Venezuelan constitution prohibits anonymity—a rule that applies to all media. The tracking of mobile phone users is an increasing problem. Since 2005, CONATEL has required mobile phone operators to collect copies of subscribers’ identity documents, addresses, fingerprints, and signatures. According to the Computer Crimes Act, this information must be delivered to state security agencies upon presentation of a judicial warrant. Service providers are also obligated to keep detailed logs of all calls, including the phone number and location of both the caller and the recipient.

---

118 Article 57 establishes freedom of expression and freedom from censorship, but also forbids anonymity. Official site of The Supreme Court: http://goo.gl/mT9okw; accessed April 15, 2014.
Despite these challenges, government opposition and independent bloggers are active on social media platforms. In 2013 and 2014, such expression was met with increased physical and technical violence extending to harassment, intimidation, detentions, and cyberattacks. Numerous fatalities were reported in the early 2014 protests, many of which appear to have been at the hands of government employees. Digital impersonations are also on the rise, and have compromised the integrity of a number of digital identities and websites.

Freedom of speech and freedom of the press are constitutionally guaranteed in Venezuela, and a 1999 provision requires the state to provide public access to ICTs. Various laws, however, have been used to undermine online freedoms and to restrict media. When coupled with CANTV's market dominance, the lack of institutional checks and balances in Venezuela makes it possible for the government to monitor and harass political opponents with impunity. Since 2001, the Supreme Court of Justice has issued no fewer than 10 judgments curbing freedom of expression, evidence of the Court's susceptibility to influence from the executive branch, particularly with regard to cases of political importance. Vague wording in the country's penal code, which criminalizes the dissemination of "false information" with prison terms of two to five years, encourages self-censorship. Article 147 of the penal code further criminalizes defamation of the president with penalties of 6 to 30 months in prison. Given that the internet is classified as a channel of mass distribution of information, some violations of the penal code—such as defamation or incitement—may be considered more severe online than in other mediums.

The Venezuelan government has historically had an antagonistic relationship with users of traditional and social media. In the summer of 2013, however, one case of censorship set precedent as the country's first formal measure forbidding a citizen from using such platforms. Judge María Lourdes Afiuni was barred from social media after using her Twitter account, @Mariaafiuni, to report on the abuse she suffered while in prison and to voice her opinion of the Venezuelan penal system. Ms. Afiuni has been held on corruption charges since making a 2009 ruling that complied with United Nations guidelines concerning unjust imprisonment, but which angered then-president Hugo Chavez. On June 15, 2013, as part of the decision that granted her parole for health reasons, a Caracas court extended a precautionary measure forbidding Ms. Afiuni from expressing herself on social media. On July 31, the Court dismissed Ms. Afiuni's appeal. While there is only one such example of court-ordered online censorship to date, it sets a disturbing precedent.

Detentions of Twitter users and citizen journalists have become increasingly common in recent years. In March 2013, after the death of President Chávez, private citizen Lourdes Alicia Ortega Perez was arrested for "spreading false information" via Twitter after making a sarcastic comment about plans for the president's funeral. She was released one week later, but is required to make monthly court

122 Gaceta Official, “Summary of the National Assembly” [in Spanish], Gaceta Oficial No. 5.763 (March 16, 2005) http://goo.gl/y8jE6g; accessed on April 30, 2014
appearances until further notice.\textsuperscript{126} In previous years, others were similarly arrested for "spreading false information" and "plotting to destabilize the government" under measures that seem designed to generate self-censorship and fear.\textsuperscript{127}

Although a positive “infogovernment law” was approved in October 2013, encouraging governmental transparency and setting the groundwork for public access to information,\textsuperscript{128} such ideals appear to function solely in theory.\textsuperscript{129} Venezuela’s Special Law against Information Crimes and its Communications Privacy Protection Law, both of which safeguard privacy and impose prison terms for those who illegally intercept others’ communications,\textsuperscript{130} are similarly overlooked when privacy breaches target members of the opposition.\textsuperscript{131} Reports have trickled in of ongoing, extralegal tapping of the phones and other private communications of key opposition figures.\textsuperscript{132}

Monitoring of the digital environment by the state is widespread and extends to both the government and the private sector. Government officials reportedly monitor members of the opposition and occasionally publish their private information as a means of intimidation. In January 2014, for example, Minister of Communication and Information Delcy Rodríguez tweeted the names, ID numbers, vacation destinations, and dates of departure of 27 opposition politicians, in a clear violation of their privacy.\textsuperscript{133} In March, Congresswoman Maria Corina Machado, who was stripped of her parliamentary seat for an alleged plot to overthrow the government, was also victim to an invasion of privacy. After slandering Ms. Machado, who was a supporter of the 2014 protests, state media obtained and aired her phone records. The complaints of Ms. Machado’s attorneys, who pointed out that interception of private communications violates the constitution, were ignored.\textsuperscript{134}

CANTV employees have been fired following the tapping of their phones, suggesting a targeted attempt by the administration to ferret out those who support the opposition and to staff the

\begin{footnotesize}

\begin{itemize}
  \item \textsuperscript{126} La Patilla, "Detienen a Tuitera por Generar Rumores Desestabilizadores" [Twitter User Was Arrested for Generating Destabilizing Rumors], March 13, 2013, \url{http://bit.ly/WnBZBY}
  \item \textsuperscript{127} Urribarri, Raisa, “El Año en que Tuiteamos en Peligro,” [The Year We Tweeted in Danger], Periodismo en Línea, November 15, 2010, \url{http://goo.gl/dyQFJA}; accessed on April 30, 2014
  \item \textsuperscript{128} Law available at the following link: http://alertalaboral.files.wordpress.com/2013/10/ley-infogobierno.pdf; accessed April 30, 2014
  \item \textsuperscript{129} Constitución de la República Bolivariana de Venezuela (Constitution of the Bolivarian Republic of Venezuela) http://goo.gl/z7FeQQA; See also: Espacio Público (Blog), “Tribunales Nieg.an Información Sobre Actuaciones de CONATEL,” [Courts Refuse Information on CONATEL’S Actions], June 13, 2013, \url{http://goo.gl/EObHOY}
  \item \textsuperscript{132} Analisis24, “Venezuela: El Ultra Secreto ‘CASO 1’ que Genero Zozobra en el Gobierno de Hugo Chávez” [The Top Secret “CASE 1” which Generated Anxiety in the Government of Hugo Chávez], January 20, 2013, \url{http://bit.ly/Wimbxq}
  \item \textsuperscript{133} Twitter account of D Rodríguez, “Trilogía del Mal-Dirigencia Opositora en Vacaciones de Lujo en el Exterior” [Trilogy of Evil-Opposition Leaders in Luxury Vacations Abroad], January 1, 2014, \url{https://twitter.com/DrodriguezMinci/status/418588045563428864}; See also: Ultimas Noticias, Minisra Rodríguez Publicó Lista de Salida al Exterior de Líderes Opositores, [Minister Rodríguez Published List of Opposition Leaders’ Trips Abroad] January 2, 2014, \url{http://goo.gl/t7d5Qx}
  \item \textsuperscript{134} El Universal, “Abogados de Machado Denunciaron a Moderadores de VTV Ante Fiscalía,” [Machado Denounced VTV Moderators to Prosecutor], March 19, 2014, \url{http://goo.gl/gfJ2bX}
\end{itemize}
\end{footnotesize}
regulator with government supporters. Members of independent and state-run media have also been subject to observation and termination based on their posts on social media. In February 2014, Globovisión journalist David De Matteis was allegedly fired from his position because of critical comments he posted on Twitter while covering a presidential press conference. During the same month, Alexander Zapata (@vozcontalento), a journalist with state-owned station VTV, was fired for criticizing the work of the Venezuelan Institute of Social Security through his Twitter account.

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. In a concerning revelation, 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.

In April 2014, the portal of the Confidential Report (reporteconfidencial.info) was raided and intelligence agents took its director, Braulio Jatar, for interrogation. Neither the authorities nor the director explained the rationale for the court-ordered raid, which involved the seizure of the site’s computers. Although Jatar was released several hours after his detention, his computers were not returned. Despite the interruption, Jatar’s YouTube channel, which covers protests and demonstrations in Tachira and Caracas, remains one of the most watched in Venezuela with more than 18,000 subscribers and more than a million views. As of June 2014, the site of Reporte Confidencial was also back up and running.

Opposition members and independent journalists who make use of Twitter have also frequently been targeted by government officials as agents of violence or instability for posts on their profiles. In July 2013, renowned journalist Nelson Bocaranda was accused of instigating a series of (fictional) attacks after posting a message about presidential election irregularities on Twitter. In December, journalist Lisseth Boon of Últimas Noticias was likewise the target of intimidation and belittling when she tweeted about the process surrounding the municipal elections.

Threats against journalists and opposition members also increased during the 2014 protests. President Maduro threatened to bring journalists and artists to court for being "agents of violence"
and for allegedly using their Twitter accounts to urge protesters to commit violent acts. The governor of Mérida likewise requested an investigation into an account, @trafficVZLA, due to its alleged role in “spread[jing] psychological attacks against the people.” Journalist Vicelyz Fadul (@vicelyz) later announced that the so-called Chavista Troop had repeatedly threatened her on Twitter because of her opinions on the protests. Lorena Arraíz (@lorenaarraiza), a journalist from El Universal who was also covering the protests, received the following message on Twitter in February: “We are going to get you and yours! Nobody is safe here.” The account responsible for the threat also displayed Ms. Arraíz’ ID number and date of birth. The aggressor’s account was deleted after complaints to various associations and the police.

In a trend that began during the protests, intelligence agents began seizing protesters’ phones in order to make organization of dissidents more difficult, to delete images and videos of the protests and of abuse of protesters, and reportedly, to analyze the data on the phones in order to identify and penetrate the opposition’s communication networks. In March, one protester died as the result of National Guard agents attempting to seize his phone. Alejandro Márquez was recording abuses of protesters when guards pursued him and brutally beat him until he surrendered his phone. Márquez, one of more than 40 protest casualties, was pronounced brain dead at the hospital.

The hacking of the websites and the accounts of opposition netizens and politicians continued to be an issue in late 2013 and early 2014. Due to the lack of any independent institution through which individuals can pursue complaints, many observers believe that the government may be directly or implicitly supporting the attacks. Although the Computer Crimes Law condemns the interception, alteration, or disclosure of any private information stored via ICTs, and specifies severe punishment for such crimes, no penalties have yet been imposed. In late 2013, a long list of opposition leaders, humorists, and writers were all victims of hacking or identity theft. According to La Patilla editor David Moran, the website of the popular independent news portal has also been victim to Distributed Denial of Service (DDoS) attacks.

In addition to the targeting of opposition websites, government accounts have also been subject to hacking in recent years. During the 2014 protests, the government blamed the opposition for the fall
of nearly 200 state websites. In February, the official Twitter account of the Maduro administration (@PartidoPSUV) was also compromised. Hackers replaced the administration's profile picture with an ironic image of late President Hugo Chávez, flanked by a photo of Bassil Da Costa, a young opposition member who was shot to death during the protests. Hackers also manipulated messages and tweeted against the government. The ruling party claimed that the Twitter attacks were intended to suspend the accounts of three Venezuelan ministers, two state media companies, two ministries, and other prominent users who sympathize with the government. The attacks were also allegedly intended to reduce the number of followers President Nicolás Maduro has on the social network. In light of these incidents, the head of state has proposed the creation of a “Bolivarian Twitter,” a social network “free from the empire and the oppression of the big corporations.” Such rhetoric is typical of the government, which often makes pronouncements to draw attention to certain issues but only sporadically follows through on its threats to create and utilize new bodies or platforms.


153 Infobae Website, “Tras la Censura a Fotos en Twitter, Hackearon la Cuenta del PSUV,” [After Censoring Photos on Twitter, PSUV Twitter Account was Hacked], February 15, 2014, http://goo.gl/3fg5b


Vietnam

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</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>28</td>
<td>28</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>33</td>
<td>34</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>75</td>
<td>76</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 89.7 million

Internet Penetration 2013: 44 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- With at least 31 behind bars, Vietnam continued to be one of the world’s worst jailers of netizens in 2014 (see Violations of User Rights).

- Article 258 of the penal code (abuse of freedoms to infringe on state interests) was increasingly used to arrest bloggers (see Violations of User Rights).

- Decree 174, in effect since January 2014, could punish antistate comments on social media with fines up to $4,700 (see Violations of User Rights).

- Sophisticated malware targeting Vietnamese activists and their supporters worldwide coincided with website blocking and blogger arrests (see Violations of User Rights).
Vietnam

Introduction

Internet freedom showed no improvement during the coverage period of this report, even as Vietnam became a member of the UN Human Rights Council in December 2013. The ruling Vietnamese Communist Party (VCP) has long feared that the internet and social media could challenge its political monopoly, but appeared more wary of international censure for its online policies in the past, notably easing harassment of digital activists between 2004 and 2006 while the country hosted an Asia-Pacific Economic Cooperation summit and joined the World Trade Organization.

The past two years saw no such moderation. While still investing in information and communication technologies (ICTs), the government has doubled the number of netizens behind bars since 2011. By 2014, Vietnam had imprisoned more bloggers than any country in the world except China. Several are serving sentences longer than a decade in conditions so poor that at least two went on hunger strike during the coverage period of this report. The legal framework for restricting online dissent has also tightened. The oppressive Decree 72 on internet management which came into effect in September 2013 intensified content restrictions for domestic internet users, but also required international internet companies to establish at least one server in the country, subject to local law and oversight. It was followed just months later by Decree 174, which threatens authors of antigovernment comments on social media with fines of US$4,700.

For some years, Vietnamese activists have been the target of sophisticated cyberattacks. In 2014, researchers found that a progovernment squad of hackers, active since 2009, targeted at least one civil society group and at least one news organization writing about Vietnam, as well as Vietnamese bloggers overseas. The malicious software used in the attacks was advanced enough to evade detection by almost all commercial antivirus programs, and sent from servers in locations around the world.

Obstacles to Access

Internet penetration was at 44 percent in 2013. Vietnam also ranked 88th on a global ICT development index, higher than regional neighbors with a larger gross domestic product like Thailand, Indonesia, and the Philippines.

Vietnam does not report figures for computer literacy, but the 93 percent overall literacy rate has helped equip the adult population to use computers. In large cities, the internet has surpassed newspapers as the most popular source for information. Wi-Fi connections are free in many urban

---

spaces such as airports, cafes, restaurants, and hotels, and city-wide in some tourist destinations. Cybercafes, though affordable for most urban dwellers, provide access for just 36 percent of internet users, and almost 90 percent of citizens can access the internet in their homes and workplaces, 2012 research shows. While access is more limited for the 70 percent of the population living in rural areas, with ethnic minorities and remote, impoverished communities especially disadvantaged, the research documented a remarkable 95 percent of citizens aged 15 to 24 with internet access nationwide. In a country where 50 percent of the population is under 30, this is a promising trend. Monthly access starts around $12 per month.

Vietnam’s mobile penetration was estimated at 131 percent in 2013, based on VNPT figures. 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 significantly in 2013, as new policies discouraged people from buying new SIM cards. Despite this, the third-generation (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.

The three biggest internet service providers (ISPs) are the state-owned Vietnam Post and Telecommunications (VNPT), which controls 63 percent of the market; the military-owned Viettel (9 percent); and the private FPT (22 percent). VNPT and Viettel also own the three largest mobile phone service providers in the country (MobiFone, VinaPhone, and Viettel), which serve 93 percent of the country’s subscriber base, while three private companies share the remainder. Informal barriers prevent new companies without political ties or economic clout from entering the market. Similarly, there is a concentration of internet exchange providers, which serve as gateways to the international internet; four out of six are state or military-owned.

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 nontransparent manner. In 2008, the MIC created the Administrative Agency for Radio, Tele-

---

9 “Điều tra biến động dân số và kế hoạch hóa gia đình thời điểm 1/4/2012” [Survey of population changes and family planning, at 1 Apr 2012], General Statistics Office, December 2012.
11 International Telecommunication Union, “Mobile-cellular Telephone Subscriptions, 2000-2013.”
16 GSMA Intelligence, “3G growth stalls in Vietnam.”
17 The four are: VNPT, Viettel, Hanoi Telecom, and VTC.
Limits on Content

Decree 72 on internet management, introduced in 2013, was the latest in a series of regulations that heavily restrict political commentary and instill self-censorship in an otherwise diverse and lively online community. It was followed by Decree 174, effective since January 2014, which threatens harsh fines for government criticism on social media. While content limits are nothing new in Vietnam, online content today is also subject to manipulation, and officials acknowledged paying commentators for the first time in 2013.

While the VCP has fewer resources to devote to online content control than its counterpart in China, authorities have nonetheless 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. Different ISPs use different techniques to inform customers of their compliance. While some notify users when an inaccessible site has been deliberately blocked, others post an apparently benign error message.

Researchers have found that Vietnamese ISPs do not block pornography. Blocking primarily targets topics with the potential to threaten the VCP’s 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 Buddhism, Roman Catholicism, and the Cao Dai religious 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, Anh Ba Sam or Dien Dan Xa Hoi Dan Su.

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.

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. The authorities are not known to have instituted restrictions on email or SMS content.

---

20 OpenNet Initiative, “Update on Threats to Freedom of Expression Online in Vietnam.”
Vietnam

The unpredictable and nontransparent ways in which topics become forbidden make it difficult for users to know what might be off-limits, and many self-censor. Bloggers and forum administrators commonly disable commenting functions to prevent controversial discussions. The party's Department for Culture and Ideology and the MPS regularly instruct online newspapers or portals to remove content they perceive as problematic. Editors and journalists who post such content risk disciplinary warnings, job loss, or imprisonment.

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. Blogging platforms were instructed to remove this “harmful” content, report to the government every six months, and provide information about individual bloggers upon request. Decree 02 followed in 2011, giving authorities power to penalize journalists and bloggers for a series of infractions, including publishing under a pseudonym. The decree differentiated between journalists accredited by the government and independent bloggers, who are allowed far fewer rights and protections.

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, extended this repressive trend, replacing “blogs” with “social networks” to encompass more online platforms. Article 5 limits overbroad categories of online activity including “opposing the Socialist Republic of Vietnam,” inciting violence, revealing state secrets, and providing false information.

Decree 72 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 also mandates that companies maintain at least one domestic server “serving the inspection, storage, and provision of information at the request of competent authorities.” Social networks are instructed to “provide personal information of the users related to terrorism, crimes, and violations of law” on request. It holds cybercafe owners responsible if their customers are caught surfing “bad” websites. It did not outline what penalties non-compliant companies could face, and how the decree might be enforced remains unclear.

Finally, in November 2013, the government issued Decree 174, which came into effect in January 2014. The decree introduced administrative fines of VND 100 million ($4,700) for anyone who “criticizes the government, the Party or national heroes” or “spreads propaganda and reactionary


26 OpenNet Initiative, “Update on Threats to Freedom of Expression Online in Vietnam.”
ideology against the state” on social media. These will be applied to offenses not serious enough to merit criminal prosecution. The decree outlined additional fines for violations related to online commerce.

Besides expanding censorship, the government has adopted new measures 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.” Some blogs which criticize high-profile party members, such as Quan Lam Bao, have attracted criticism for reflecting internal power dynamics rather than objective opinion.

Despite government restrictions, Vietnam’s internet is vibrant and offers a diversity of content in the Vietnamese language. YouTube, Twitter, and international blog-hosting services such as Blogger or WordPress are freely available and growing in popularity. Facebook, which faced sporadic—and officially unacknowledged—blocks in 2010 and 2011, was largely accessible in 2014, though still required circumvention tools to access in some cases. Facebook overtook local competitor Zing for the first time in 2012, and had more than double the number of Vietnamese subscribers by May 2013.

Although most blogs and social media pages address 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. Websites such as Anh Ba Sam, Que Choa or Bauxite Vietnam react quickly to sociopolitical events and were influential in mobilizing demonstrations in Hanoi and Ho Chi Minh City against China’s claim to the Paracel and Spratly Islands in 2011. In 2012, blogs played an important role in rallying public opinion and providing evidence against local authorities who seized agricultural land from farmers. In 2013, LGBT activists used social media to show support for same-sex marriage.

Violations of User Rights

Over the last five years, Vietnam has subjected bloggers and online writers to interrogation, imprisonment, and physical abuse, a repressive trend that intensified in 2013 and 2014. Sentences handed down in cursory trials, which are often closed to the press, are getting longer. Three bloggers were detained under Article 258 of the penal code—abusing freedom to threaten the state—within the space

30 “71.4% người dùng Internet tại Việt Nam sử dụng Facebook” [71.4% Internet users in Vietnam use Facebook], ICT News, September 23, 2013, http://ictnews.vn/Internet/71-4-nguoi-dung-internet-tai-viet-nam-su-dung-facebook-111922 ICT.
Vietnam

of two months in mid-2013. Hackers have targeted Vietnamese antigovernment activists since 2009. In 2014, analysis of recent cyberattacks showed them diversifying targets as well as technology to suppress criticism of the Vietnamese state, and increasingly combining with more openly acknowledged official tactics like online manipulation and website blocking.

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 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. 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.

Reporters Without Borders counted 31 netizens imprisoned in Vietnam as of April 2014, compared to 17 in 2011. This significant jump was fuelled by a January 2013 court ruling that found 14 Catholic students, bloggers, and human rights activists guilty of subversion under Article 79, in part for their online activities. The sentences ranged from 3 years in prison followed by 2 years under house arrest to 13 years’ imprisonment and 3 years’ house arrest.

Sentences continued to be passed during the coverage period. In May 2013, two students, Nguyen Phuong Uyen, 21, and Dinh Nguyen Kha, 25, who were arrested in October 2012 for disseminating antigovernment materials in public places and online, were jailed for 6 and 8 years respectively. Citing the indictment, Reporters Without Borders said they had been accused of contact with an overseas dissident over Facebook. An appeals court later reduced the sentences to 3 years’ probation for Uyen and 4 years’ imprisonment for Kha. Lawyer and blogger Le Quoc Quan, who was arrested in December 2012 shortly after the BBC Vietnamese service published one of his articles on its website, was sentenced in October 2013 to 30 months in prison and a fine of VND 1.2 billion ($57,000) for tax evasion, a charge frequently trumped up by the government to silence dissidents.

---

Arrests were also ongoing, particularly under Article 258. Police arrested blogger Truong Duy Nhat in May 2013.\(^ {42} \) Two arrests on the same charge followed in June, targeting the prominent 61-year-old Pham Viet Dao, who wrote about sensitive issues such as the territorial disputes with China,\(^ {43} \) and blogger Dinh Nhat Uy, who is Dinh Nguyen Kha’s brother.\(^ {44} \) In October, after a four-hour trial, Uy was sentenced to one year on probation.\(^ {45} \) In March 2014, Pham Viet Dao was sentenced to 15 months in prison;\(^ {46} \) Truong Duy Nhat was given two years.\(^ {47} \) On May 5, 2014, blogger Nguyen Huu Vinh, who writes Anh Ba Sam, was arrested on the same charge.\(^ {48} \)

Two of the longest-serving bloggers went on separate hunger strikes during the coverage period of this report to protest against their prison conditions. Nguyen Van Hai, who writes under the pen name Dieu Cay (“Peasant’s Pipe”) was kept in detention after completing a two and a half year prison term for alleged tax evasion in 2010, then sentenced to an additional 12 years in prison and 5 years under house arrest for “activities against the government” in 2012.\(^ {49} \) Through his blog, he has been a vocal critic of the government’s human rights record and an advocate for Vietnamese sovereignty over the Spratly Islands. He refused to eat for more than a month in July 2013 until authorities agreed to investigate his petitions protesting abusive treatment.\(^ {50} \) The New York-based Committee to Protect Journalists honored him in absentia with an International Press Freedom Award in October 2013.\(^ {51} \) Another vocal online dissident, Cu Ha Huy Vu, went on hunger strike for three weeks in June. He is serving a sentence of seven years in prison and three years house arrest handed down in a 2011 trial that was closed to the public.\(^ {52} \) He was released early in April 2014.\(^ {53} \)

In addition to imprisonment, bloggers and online activists have been subjected to physical attacks, job loss, severed internet, travel restrictions, and other rights violations. During the coverage period of this report, several bloggers were harassed for organizing and participating in public events, including a series of incidents in May 2013. Police in Hanoi, Nha Trang, and Ho Chi Minh City beat bloggers who took part in picnics around the country, arranged via Facebook for people interested

---


in human rights. In Saigon, blogger Nguyen Hoang Vi documented her mother and sister’s facial abrasions after police attacked their picnic. In May, at least one internet user attending a dissident trial reported on Facebook that an officer outside the court punched him in the chest. The same month, blogger Huynh Ngoc Chenh, recipient of the 2013 Global Netizen Prize from Reporters Without Borders and Google, was denied permission to leave the country. Beatings and harassment continued in Ho Chi Minh City in December 2013 during a celebration of International Human Rights Day.

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 2014, however, the registration process is not linked to any central database and could be circumvented using fake ID.

Decree 72 requires all providers—and social networks in particular—to provide user information to “competent authorities” on request, but lacks procedures or oversight to discourage intrusive registration or data collection. 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 coming years.

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 such as contacts, text messages, and emails without per-

---

56 Reporters Without Borders, “Appeal Court Upholds Jail Time For Five Bloggers.”
62 “Decree No. 72/2013/ND-CP.”
mission from other computers. Citizen Lab noted that the presence of such a server did not prove who was running it, though it is marketed to governments.

Activists in Vietnam and abroad have been the target of systematic cyberattacks since 2009. When their activity was first documented, 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 attacking 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.

Since then, the hackers’ methods have evolved, though their targets remain the same. 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. In January 2014, researchers revealed that at The Associated Press newswire and the U.S.-based nonprofit Electronic Frontier Foundation had also been targeted—for coverage of Vietnam—by malicious hackers spending “tens of thousands of dollars” to launch attacks from servers around the world. Analyzing the suspicious emails, the California-based Electronic Frontier Foundation said the group responsible appeared to have been operating since late 2009, though their malware was advanced, detectable by only one of nearly fifty antivirus vendors.

Attacks sometimes coincide with abusive comments debasing the site’s content, a hallmark of manipulated online discourse, but not traceable to state actors. In the past year, they corresponded with more official controls such as website blocking and arrests. A California-based blog was hacked in 2013. Once the owner, Ngoc Thu, regained control of the site and moved it to a different URL, it was blocked by ISPs. Blogger Truong Duy Nhat’s website became briefly inaccessible after his arrest in May 2013. When it reappeared, the blog automatically installed malware on visitors’ devices, targeting a self-selecting audience of his supporters for surveillance and future cyberattacks.

---


70 Chris Brummit, “Vietnam’s Cyber Troops’ Take Fight to US, France.”

Zambia

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Freedom Status</td>
<td>N/A</td>
<td>Partly Free</td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>n/a</td>
<td>12</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>n/a</td>
<td>13</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>n/a</td>
<td>18</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>N/A</td>
<td>43</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 14.2 million

Internet Penetration 2013: 15 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- In July 2013, Zambia’s southwestern region, Barotseland, reported an area-wide power outage that impacted all internet and mobile services for about 40 minutes. The region’s critical online radio station accused the government of deliberate interference to censor a controversial radio show (see Obstacles to Access).

- Access to four independent news websites was blocked for the first time in Zambia, reportedly as part of the government’s overall crackdown on critical media coverage (see Limits on Content).

- The ruling party continued to stall on a new draft constitution that provides for electronic media freedom and explicitly prohibits the government from interfering with media activities. The government instead called for legislation to regulate online media, citing the problems of “internet abuse” and cybercrime (see Violations of User Rights).

- The regulator disconnected all unregistered SIM cards after the registration deadline of January 31, 2014 (see Violations of User Rights).

- Officials targeted individuals suspected of being associated with the critical online news outlet Zambian Watchdog, arresting three suspects (see Violations of User Rights).
Editor’s Note:

President Michael Sata died while holding office on October 28, 2014, leaving Vice President Guy Scott as Acting President for 90 days before the country holds a presidential by-election as required by the Constitution. The events covered in this report reflect developments during the May 1, 2013 – May 31, 2014 coverage period that occurred before President Sata’s death. A draft constitution was eventually released in October 2014, though its path forward remains unclear amid the country’s political transition.

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. Liberalization of the information and communication technology (ICT) sector in 1994 enabled new players to enter the market and invest in ICT development, but a long period of economic decline and stagnation through the late 1990s hindered meaningful progress. In recent years, investment in ICTs has regained momentum, bolstered by economic growth and government support through measures such as the 2009 National ICT Policy, the Information and Communications Act of 2009, and the Electronic Communications and Transactions (ECT) Act No. 21 of 2009, all of which established a new institutional, legal, and regulatory environment for ICT development.

Meanwhile, political stability in Zambia has been tenuous over the past few decades, with different ruling governments restricting freedom of expression and press freedom to varying degrees. 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 in the following years 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. The government had previously tried to ban one of the outlets, Zambian Watchdog, in 2012.

Since coming into power in September 2011, the PF government intensified its crackdown against the press, using both legal and extrajudicial measures ostensibly to punish journalists for critical media coverage. In 2013, the authorities specifically targeted the independent online outlet Zambian Watchdog, which is based abroad but employs anonymous journalists in the country. Shortly after Zambian Watchdog was blocked in July 2013, officials raided the homes of two journalists suspected of writing for the outlet and arrested them for allegedly possessing seditious and obscene materials. Surveillance became a widespread concern during the coverage period, as SIM card registration

---

requirements led to beliefs that the government wanted to keep tabs on Zambians’ mobile communications. There were reports throughout 2013 and 2014 of the government targeting various individuals with phone tapping, from senior government officials who fell out of Sata’s favor to civil society leaders. In September 2013, China’s Huawei Technologies was accused of installing email hacking devices on all ISPs in Zambia.

**Obstacles to Access**

Access to ICTs in Zambia has spread steadily over the past decade, with the internet growing from a penetration rate of 2 percent in 2004 to over 15 percent in 2013, while mobile phone penetration grew from 4 percent in 2004 to nearly 72 percent in 2013, according to the International Telecommunication Union (ITU). Both fixed-broadband and mobile broadband subscriptions are still extremely rare, however, with low penetration rates of 0.1 percent and 0.7 percent, respectively, in 2013.

Internet infrastructure is poorly developed in rural areas, resulting in a significant urban-rural divide in access. As such, rural citizens typically access the internet from telecenters or cybercafes, though the expansion of mobile phone internet services in recent years has enabled more people to access the internet from home, resulting in a declining number of internet cafes. Nevertheless, the cost of internet services in Zambia is still expensive for the majority of the population, largely due to its landlocked position, which makes the country reliant on satellite links or interconnection agreements with neighboring countries. As of mid-2014, a monthly subscription for fixed-line broadband internet costs an average of US$128, which is completely out of reach for the 10 million Zambians who live on less than US$2 per day. Meanwhile, low-income Zambians must spend at least 35 percent of their incomes for subscriptions to mobile broadband services, according to a 2013 study by the Alliance for Affordable Internet (A4AI).

Meager electricity and the high cost of electronic devices further limit access to ICTs in rural areas, where only 3.5 percent of households have access to electricity. Rural communities are particularly vulnerable to the practice of load shedding, which shuts off electricity service in one area to support demand in another region, typically urban areas. Lasting anywhere between 5 minutes and 48 hours, power outages regularly interrupt internet and mobile phone services and limit internet connectivity by making local equipment unstable after a power failure.

---


Zambia

In July 2013, the southwestern region of the country known as Barotseland—which has been fighting for its rights to autonomy within Zambia since 1964—reported a region-wide power outage that impacted all internet and mobile services for about 40 minutes. The regional independent online news outlet, Barotse Post, accused the government of deliberately disconnecting the region’s electricity during an anticipated online live chat forum that was scheduled to discuss the government’s abrogation of a 1964 agreement that had granted Barotseland its autonomy. While the government’s alleged connection to the region-wide power outage could not be confirmed, the disruptive power outage demonstrated how the lack of reliable electricity regularly impacts citizens’ access to ICTs and information.

Meanwhile, internet connection speeds in Zambia are slow, averaging 1.3 Mbps (compared to a global average of 3.9 Mbps), according to May 2014 data from Akamai’s “State of the Internet” report. In addition, Zambia’s broadband adoption rate (characterized by connection speeds greater than 4 Mbps) was less than 2 percent of the internet population, while the country’s narrowband adoption rate (connection speed below 256 kbps) was about 9 percent.

The Zambian ISP market is very competitive, characterized by a lack of a significant dominant player. As of 2014, there are 23 internet service providers, three of which are also Zambia’s mobile phone providers: MTN, Airtel, and Zambia Telecommunications Ltd (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 President Sata, who “deemed it desirable and expedient to compulsorily acquire the 75 percent shareholding of [Libya’s] Lap Green Network in Zamtel,” according to the government’s official press release.

---

10 According to the Unrepresented Nations and Peoples Organization (UNPO): “Barotseland was a protectorate under British colonial rule and became part of Zambia at the country’s independence in 1964. Barotse representatives signed the Barotseland Agreement 1964, whose purpose was to transfer Barotseland from British to Zambian protection. Therefore, the Agreement presented the Barotse autonomy within independent Zambia, whose only role would be to protect and safeguard Barotseland while receiving the benefits of strong political and economic ties. Zambia was supposed to inherit Britain’s obligations over Barotseland, but instead chose to incorporate Barotseland into the newly formed Republic of Zambia. The Barotse people wish to regain their autonomy by exerting their right to self-determination and self-governance. They were incorporated into Zambia by a violation of the Barotseland Agreement 1964 and wish for this to be recognized by international institutions.” See: UNPO, “Barotseland,” March 27, 2014, http://unpo.org/members/16714.


percent share of Zamtel to Lap Green in 2010 for US$257 million.18 Nevertheless, Zamtel has the smallest share in the mobile phone market,19 and there are plans for a fourth mobile operator to enter Zambia in 2015.20 On the other hand, Zamtel commands the largest market share of internet subscriptions, with 61 percent of the market, as of the latest data available from February 2013.21

As a landlocked country, Zambia’s national fiber backbone is provided by three operators—Zamtel, the state-owned Zambia Electricity Supply Corporation Ltd (ZESCO), and the Copperbelt Energy Corporation (CEC)—while Zamtel operates the fiber-optic connection to two international submarine cables—the West Africa Cable System (WACS) and South Atlantic 3 (Sat-3).22 MTN and Airtel lease access to the undersea cables from Zamtel,23 though MTN also connects to the Eastern African Submarine Cable System (EASSy).24 According to the ITU, the gateway to the international internet in Zambia is fully liberalized and competitive.25 In July 2013, however, the critical online news outlet Zambian Watchdog reported details from inside sources alleging that the president’s office controls Zambia’s internet exchange point, which is housed in the same building as state-owned Zamtel in the capital city Lusaka.26 Zamtel’s management of two of the country’s international submarine cables may also give the government some level of control over the international gateway.

In the past, political interference in the ICT sector has obstructed the existence of diverse business entities providing access to digital technologies in Zambia. For example, in 2008, the government stripped the South African operator Vodacom of its provisional license to set up operations in Zambia, reportedly in an effort to protect the state-owned Zamtel.27 Later in December 2009, the government issued a statutory instrument prohibiting the entry of new providers in the mobile service market until 2015,28 which effectively restricted the number of players to three: state-owned Zamtel, Zain (purchased in 2010 by Airtel), and MTN.29 Industry observers believed that the moratorium on new mobile providers was intended to enable the state-owned Zamtel to increase

its market share and value before its subsequent privatization in 2010.\textsuperscript{30} In recent years, there have been no further reports of political obstruction in the ICT sector. At the time of writing, the 2009 statutory instrument restricting the number of mobile providers is set to expire in December 2014, and there are plans for a fourth provider to enter the market in 2015.\textsuperscript{31}

The Information and Communication Technologies (ICT) Act of 2009 provides for the economic and technical regulation of ICTs in Zambia. The Act also established the Zambia ICT Authority (ZICTA) as the sector regulator, which the ITU has characterized as autonomous in its decision-making.\textsuperscript{32} Nevertheless, the minister of communications is still mandated to oversee ZICTA’s activities and is responsible for appointing the members and chairperson of the ZICTA’s board.\textsuperscript{33} The minister is also entitled to issue general directives, which the regulator is obligated to carry out.\textsuperscript{34}

**Limits on Content**

During the coverage period, four independent news websites were blocked—two popular outlets based abroad, and two radio news websites from the Barotseland region of the country. Reports indicated growing government intentions to manipulate online content, and self-censorship seemed to increase following a coordinated crackdown on critical online news.

In 2013, access to independent news websites was blocked for the first time in Zambia, reportedly as part of the government’s overall crackdown on critical media coverage. *Zambian Watchdog*—an independent news site based abroad with anonymous reporters on the ground and known for its critical reporting on the ruling Patriotic Front party—was the first website to be blocked on June 24, 2013.\textsuperscript{35} A secure version of the website using the “https” protocol was created four days later but was subsequently blocked on July 16, followed by the site’s renamed domain at Zwd.cums.in.\textsuperscript{36} Reporters Without Borders worked swiftly to create a mirror site for *Zambian Watchdog* at Zambianwatchdog.rsf.org, which was blocked within three hours on July 18.\textsuperscript{37} Despite the persistent blocking efforts, *Watchdog* content could still be accessed via proxies and the news outlet’s Facebook page.

There is no concrete evidence that the government was behind the blocking of *Zambian Watchdog* and its affiliated mirror websites, though testing conducted by an independent researcher with the Tor Project’s Open Observatory of Network Interference (OONI) in July 2013 discovered the presence

\textsuperscript{33} First Schedule (Section 4), The Information and Communication Technologies, Act [No. 15 of 2009], http://www.zicta.zm/index.php?option=com_jdownloads&Itemid=79&view=finish&cid=186&catid=24&m=0.
of deep packet inspection (DPI) filtering tactics as the source of the block.\textsuperscript{38} Watchdog accused Chinese company Huawei Technologies of installing DPI on Zambia’s ISPs to enable the blocking of internet content.\textsuperscript{39} 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.\textsuperscript{40} He also characterized the party responsible for the blocking as a “well-wisher” and thanked them for their work.\textsuperscript{41}

In addition, the Patriotic Front government has targeted Zambian Watchdog since at least 2012, when the minister of tourism publicly called for the outlet to be banned, ostensibly out of concern that Watchdog’s critical reporting would negatively impact the country’s image in the lead up to Zambia’s hosting of the UN World Tourism Organization meeting in August 2013.\textsuperscript{42} The minister reportedly directed the regulatory authority ZICTA to “revoke the law that allows the Zambia Watchdog to operate as an online publication,” which ZICTA declined to do since the website is not hosted within the country’s jurisdiction.\textsuperscript{43} In May 2012, Zambian Watchdog was also a target of distributed denial of service (DDoS) attacks that temporarily brought the site down,\textsuperscript{44} which the site blamed on the government.\textsuperscript{45}

In July 2013, another critical online publication hosted abroad, Zambia Reports, was completely blocked inside the country. The news site filed a complaint to ZICTA about the block on July 22 but received no response.\textsuperscript{46} Administrators subsequently sent a letter to the Ministry of Information and Broadcasting Services on July 23 asking for an explanation of the reasons for the blocking and called for a national enquiry into online censorship, which also received no acknowledgment.\textsuperscript{47} In September 2013, access to the online news outlet Barotse Post and the online radio station Radio Barotse—two websites that advocate for an autonomous Barotse state in western Zambia—were blocked. Similar to the other censored news sites, content could still be accessed via proxies and the webpages’ social media accounts.\textsuperscript{48}

In April 2014, Zambia Reports announced that both Zambian Watchdog and Zambia Reports

were unblocked, ostensibly due to pressure from international partners. Nevertheless, there is a complete lack of transparency behind censorship decisions, in addition to an ineffective complaints and appeals process through the regulatory body ZICTA, as demonstrated by the government's silence toward Zambia Report's formal complaint to the regulator and ministry of information in July 2013. Otherwise, social media platforms such as Facebook, Twitter, and YouTube and international blog-hosting services are all freely available in Zambia.

The government also censors the internet by directing websites to take down certain content upon request, though the extent of this practice is unknown given the predominance of state-owned and progovernment news outlets in the country. The majority of takedown requests are likely unreported. 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 prohibited content under the 2009 Electronic Communications and Transactions Act.

Government pressure on the media since President Sata took office in 2011 has created a climate of intimidation and increased self-censorship among journalists, both online and off. Social media users tend to express themselves freely online, but a growing belief that the government monitors social media activity has made general users more cautious in recent years. Nevertheless, the Zambian blogosphere is vibrant, representing a diversity of viewpoints and opposition voices, and many mainstream journalists have turned to blogs to express themselves more freely. These journalist bloggers and many others, however, choose to write anonymously due to the threat of harassment, legal action, or both, particularly on issues regarding the Patriotic Front government and corruption. Online self-censorship increased palpably following the arrests of journalists for their suspected connection to Zambian Watchdog in summer 2013 (see “Violations of User Rights”).

In response to the growing influence of independent online news outlets and blogs, the ministry of information in September 2013 reportedly directed public media houses to expand their presence on the internet and engage with audiences on social media. According to the Media Institute of Southern Africa (MISA), the public outlets were also instructed to provide only “correct” information about Zambia, reflecting the government’s intent and efforts to manipulate online content.

Moreover, 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.

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. In addition, private companies often do not advertise in news outlets that seem antagonistic to government policies out of fear of 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.

Despite the blocking of Zambian Watchdog and Zambia Reports in 2013, Zambian netizens were largely still able to access the websites through the use of proxies. Netizens also increasingly took to the internet as a platform for digital activism. Most notably in July 2013, a collective known as the Zambian Bloggers Network organized a demonstration at the Freedom Statue in Lusaka to protest internet censorship and the arrests of journalists suspected of their connection to Zambian Watchdog. Unfortunately, the turnout was small—likely due to fears of how the government would respond—and the demonstration had little impact on the status of the blocked websites and arrested journalists.

Violations of User Rights

The ruling party continued to stall on a new draft constitution that provides for electronic media freedom and explicitly prohibits the government from interfering with media activities. The regulator disconnected all unregistered SIM cards after the registration deadline of January 31, 2014. Officials targeted individuals suspected of being associated with the critical online news outlet Zambian Watchdog, arresting three suspects.

Freedom of expression is enshrined in the Zambian Constitution but is limited by other statutes that restrict expression in the interest of defense, public order, safety, morality, and health, which can be broadly interpreted. Meanwhile, the constitution does not explicitly guarantee press freedom but includes a provision stating that “no law shall make any provision that derogates from freedom

---

of the press." Some media observers have noted that this provision inadequately protects press freedom. Freedom of expression and the media are further limited by clauses in the penal code that criminalize defamation of the president and gives 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.

In an effort to deliver on its campaign promise of tackling legal reform, the Patriotic Front government in September 2011 tasked a coalition of government and civil society members with drafting a new constitution. Completed in late 2013, the final draft (which the president tried to keep from the public but was leaked by Zambian Watchdog in January 2014) included specific protections for print, broadcast, and electronic media freedom and explicitly prohibited the government from exercising control or interfering with media activities. In April 2014, however, President Sata reportedly rejected the draft constitution altogether, proclaiming that the process had been “hijacked by individuals whose objective is to embarrass, humiliate and undermine the public will” and that “the country already has a functional constitution.” Despite the president’s objections, the draft constitution is still being deliberated as of late 2014, pushed forward by Justice Minister Edgar Lungu who published the draft online in October 2014 for public review.

Judicial independence is guaranteed in the constitution but is not respected in practice and is 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. Upon taking office in 2011, Sata suspended top judges for alleged misconduct and installed his cousin as acting chief justice.

In 2013, the Patriotic Front government intensified its crackdown against the press, using both legal and extrajudicial measures ostensibly to punish journalists for critical media coverage. The authorities specifically targeted the independent online outlet *Zambian Watchdog*, which is based abroad but employs anonymous journalists in the country. On July 9, 2013, shortly after *Zambian Watchdog* was blocked, officials raided the homes of two journalists suspected of writing for the outlet—Clayson Hamasaka and Thomas Zymbo—purportedly to search for seditious materials and drugs. The authorities confiscated computers and other digital equipment, then detained and interrogated the two individuals without charge for nearly two days. Zymbo was charged a few days later with sedition for his alleged possession of seditious documents about President Sata found in his home. Hamasaka was initially released without charges but rearrested a few weeks later for the alleged possession of obscene material that was reportedly found on his confiscated laptop.

Another journalist suspected of working for *Zambian Watchdog*, Wilson Pondamali, was arrested on July 16, 2013 and held for two weeks without bail on charges of “unlawful possession of restricted military pamphlet” based on a document the police allegedly found in his home suggesting that President Sata was not fit to govern. He was also charged with stealing a library book but later acquitted of the ridiculous charge in August 2014, though his previous charge remained. All cases against the suspected Watchdog journalists remained resolved as of mid-2014.

Similar in fashion to the *Zambian Watchdog* crackdown, the police arrested three people on September 9, 2013 for possession of “seditious” news articles they had allegedly downloaded from the online news outlet *Barotse Post*, which was blocked just a few days prior to the arrests. One individual was shortly released while the two others remained in detention, though no further information about the individuals and the status of their charges were known as of mid-2014.

---

The ability for Zambians to communicate anonymously through digital media is compromised by SIM card registration requirements, which were instituted in September 2012 and extended to January 31, 2014, after which point the regulator ZICTA disconnected all unregistered SIM cards.

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. While the government stated that the registration requirements were for the purposes of combatting crime, 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.

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.

Meanwhile, 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. 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.” This provision may have enabled the government to order ZICTA to shut down Zambian Watchdog in 2012, which the regulator ultimately could not do since the website was not hosted in the country. The .zm domain was previously managed by Zamnet.

The Electronic Communications and Transaction Act of 2009 also details conditions for lawful interception of communications, which generally requires a court order. Since Sata came into office in September 2011, however, numerous reports have accused the government of conducting extensive illegal surveillance of citizens’ ICT activities. There were reports throughout 2013 and

---

2014 of the government targeting various individuals with phone tapping, from senior government officials who fell out of Sata’s favor to civil society leaders.

In February 2013, Zambian Watchdog reported that the government had contracted Chinese experts to install an internet surveillance system such as deep-packet inspection (DPI) technology to 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 DPI technology as the mechanism behind the blocking. Zambian Watchdog also separately reported that Sata had signed a presidential order in February 2013 that authorized the president’s office to interfere with ICT communications without oversight. 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.” Later in September 2013, Zambian Watchdog reported that China’s Huawei had installed email hacking devices on all ISPs in Zambia. To date, Zambian Watchdog has been the primary source of reports on illegal surveillance in Zambia.

In the past few years, journalists noted an increasing climate of intimidation for media workers who regularly faced harassment and physical attacks for their independent reporting. In 2013, violence extended to online journalists. In its attempts to shut down the critical online news outlets, Zambian Watchdog and Zambia Reports, the government targeted individuals suspected of writing for the outlets anonymously, including Thomas Zyambo, Clayson Hamasaka, and Wilson Pondamali who were all harassed and subsequently arrested between June and September 2013. Zyambo was reportedly threatened and physically assaulted by President Sata’s son for unknown reasons in March 2014, while Pondamali was attacked in April 2014 at a public event, allegedly by government “thugs” who took off with his digital equipment.

Otherwise, 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. Zambian Watchdog last reported a DDoS attack against its website in May 2012, which brought

---


down the site for about eight hours.\textsuperscript{102} In April 2014, the Media Institute for Southern Africa (MISA) was reportedly hacked, alongside a number of government websites, by hackers from the Middle East.\textsuperscript{103}


Zimbabwe

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partly Free</td>
<td></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>14</td>
<td>15</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>54</td>
<td>55</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 13 million

Internet Penetration 2013: 19 percent

Social Media/ICT Apps Blocked: No

Political/Social Content Blocked: Yes

Bloggers/ICT Users Arrested: Yes

Press Freedom 2014 Status: Not Free

Key Developments: May 2013 – May 2014

- General elections took place in July 2013, which President Robert Mugabe’s ZANU-PF party overwhelmingly won. In the week leading up to the elections, the telecommunications regulator issued a directive to mobile phone providers to block the dissemination of bulk SMS messages (see Introduction and Limits on Content).

- An anonymous Facebook user, using the pseudonym Baba Jukwa, continued to incite the ruling party, reportedly leading President Mugabe to post a US$330,000 reward in July 2013 for any individual willing to unmask the elusive whistleblower (see Limits on Content).

- A new constitution was adopted in May 2013, providing for press freedom and freedom of expression (see Violations of User Rights).

- Two ordinary Facebook users were arrested for their posts, one for alleging that President Mugabe had died, the other for posting an image of an electoral ballot displaying a vote for opposition candidate, Morgan Tsvangirai (see Violations of User Rights).

- Mass surveillance and illegal interception activities by security agencies reportedly increased following the July elections, for both national security and politically motivated purposes (see Violations of User Rights).

- The Postal and Telecommunications (Subscriber Registration) Regulations, enacted in October 2013, expanded the scope of subscriber registration requirements to broadly include all telecommunications services and provided the authorities with access without a court order (see Violations of User Rights).
Zimbabwe

Introduction

In 2013, a new constitution that somewhat improved media and freedom of expression rights was passed in a referendum and signed by President Robert Mugabe in May, while on July 31, a general national election was held, keeping President Mugabe and the ruling ZANU-PF party in power with a supermajority. During these events, the internet was a key platform for citizen discussions and engagement on political issues. The constitutional referendum and general election became the most internet-fueled political contests to date, as citizens, political parties, and civil society took to the net to campaign for their positions, policies, and platforms. Contestations over the election results also played out on the internet, with many images and discussions of alleged vote rigging posted on social media platforms such as Facebook, Twitter, and YouTube.

The July 2013 general elections also served as a basis for many internet freedom violations in Zimbabwe during the coverage period. For example, in the lead-up to the elections, an independent community radio station reported frequent internet disconnections in its office, and internet cafe owners reported slow internet connectivity. The dissemination of bulk SMS messages was banned prior to the election, with the exception of bulk SMS messages from the ruling ZANU-PF. Various ruling party officials frequently expressed a desire and intent to increase control over ICTs throughout the year, such as the proclamation made during the party’s annual conference in December 2013 that called for the blocking of foreign-based radio stations that are broadcast over the internet. Meanwhile, the anonymous Facebook user, Baba Jukwa, continued to goad the ruling party since his or her appearance in March 2013, reportedly leading President Mugabe to post a US$330,000 reward in July 2013 for any individual willing to unmask the elusive whistleblower.

A crackdown on user rights intensified in 2013 following the July elections, beginning with reports of increasing surveillance by the Central Intelligence Organization (CIO) in an effort to stem potential post-electoral unrest. Two ordinary Facebook users were arrested for their posts, one in July for posting an image of an electoral ballot displaying a vote for the opposition candidate, Morgan Tsvangirai; the other in January 2014 for alleging that President Mugabe “had died and was being preserved in a freezer.”

Mass surveillance and illegal interception activities by security agencies reportedly increased following the July elections, for both national security and politically motivated purposes. On October 1, 2013, the government enacted a new so-called “spy law” known as the Postal and Telecommunications (Subscriber Registration) Regulations, which expanded the scope of subscriber registration requirements previously limited to SIM cards to broadly include all telecommunications services. In addition to requiring providers to avail law enforcement officers with copies of their subscriber registers upon request without a court order, the “spy law” established a Central Subscriber Information Database, which POTRAZ can access to “assist law enforcement agencies on safeguarding national security.” The Parliamentary Legal Committee (PLC) declared the new regulations unconstitutional in March 2014, leading to an amended version enacted in July 2014 that provided for judicial oversight but left open a loophole for abuse.

Obstacles to Access

Zimbabwe's internet access has continued to expand steadily, growing from a penetration rate of 17 percent in 2012 to nearly 19 percent in 2013, according to estimates by the International Telecommunication Union (ITU).\(^2\) By contrast, official government statistics report an internet penetration rate of 42 percent in December 2013, up from 30 percent in 2012,\(^3\) though the government's data includes both fixed-line and mobile internet subscriptions, the latter of which comprise over 98 percent of all internet subscriptions.\(^4\) The ITU reported a mobile broadband penetration rate of 38 percent in 2013.\(^5\)

The sector’s rapid growth can be attributed to widespread mobile phone penetration, which stood at 96 percent in 2013, per ITU statistics, while government reports noted a mobile penetration rate of 104 percent as of December 2013.\(^6\) Service providers have indicated that Zimbabwe has reached mobile phone saturation levels, enabling them to provide enhanced services such as mobile banking and mobile internet.

Similar to most countries in Africa, Zimbabwe benefits from low-cost, internet-enabled imitation mobile phones from Asia. Internet access on mobile phones has been further facilitated by the introduction of 3G, 4G, and EDGE technology in the past few years.\(^7\) The decreasing price of mobile internet access—which dropped from US$1.50 per megabyte (MB) in 2011 to US$1 per MB as of April 2014—has also facilitated increased access. Subscription fees for 3G services cost US$30 per month for 10 GB, and other service providers offer 3G services on a pay-as-you-go basis for as little as $0.10 per MB.\(^8\)

Meanwhile, competition within the sector has generally forced prices for mobile broadband and Wi-Fi to decrease from US$75 for 20 MB to US$59 for speeds of up to 1 Mbps.\(^9\) In October 2013, Econet introduced a Facebook mobile package that allows its subscribers to access Facebook through special data bundles for as little as US$0.95 per week or US$3 per month.\(^10\) Zimbabwe is estimated

---

8 As of mid-2014, ISP, data and VoIP provider service, Africom offers 4GB for $25. Mobile telephony company Telecel offers a promotional mobile phone internet data for $0.11 cents unlimited use per day, and state fixed telephone operator, TelOne, offers bandwidth for $61 per month for 15GB through fixed line phone services and wireless devices.
Zimbabwe

to have 1.2 million Facebook users, and with Econet being the market leader, this promotion is set to enhance access and use of the social media platform.

Despite the increasing number of users, access to the full range of internet services via computers remains expensive for many Zimbabweans whose households earn an average monthly income of approximately US$180, though market competition among service providers is slowly bringing down prices. For example, the cost of wireless 3G modems has remained steady at US$30 and is accessible on prepaid wireless access devices. In the past year, the state-owned fixed-line operator TelOne cut its internet access costs from US$30–$40 per month (including installation fees) to $25. Computer prices have maintained a steady price of an average of US$350 and $450 in 2013, with some promotions selling laptops at US$250.

Although competition has decreased the cost of internet access, effective broadband for home and individual users has not been fully realized due to the poor infrastructure of the state-owned TelOne. In 2013, fixed broadband subscriptions remained low at approximately 103,500 subscriptions, with broadband penetration increasing slightly from 0.5 percent in 2012 to 0.7 percent in 2013. Nevertheless, TelOne worked to extend ADSL broadband services across the country throughout 2013, reaching almost all small towns across the country, and providing broadband to its clients through a prepaid service. Meanwhile, Econet launched its 4G network in August 2013, which has a speed of 65 Mbps—10 times faster than the current 3G network—and costs US$90 for access via a USB modem.

Despite increasing access to broadband, internet speeds are still slow, averaging 1.7 Mbps (compared to a global average of 3.9 Mbps), according to May 2014 data from Akamai’s “State of the Internet” report. In addition, Zimbabwe’s broadband adoption (characterized by connection speeds greater than 4 Mbps) was about 7 percent of the internet population, while the country’s narrowband adoption (connection speeds below 256 kbps) was over 8 percent.

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. Nonetheless, there remains a significant urban-rural divide in access to both internet and mobile technologies, particularly as a result of major infrastructural

---

18 From research via calls to relatives and friends who live near rural business centers as well as personal visits to some rural centers.
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. Power outages affect both households and business entities such as cybercafes, while prolonged power blackouts often affect mobile telephony signal transmission equipment, resulting in cutoffs of both mobile networks and internet connections.

Zimbabwe currently has 12 licensed internet access providers (IAPs) and 28 internet service providers (ISPs), the former of which offer only internet access while ISPs may provide additional services. Of the 12 IAPs, 11 have Class A licenses which allow them to offer VoIP services in addition to public data and internet service. ISP connections remain constrained by the limited infrastructure of IAPs through which they must connect. As set by POTRAZ the license fees for IAPs and 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 POTRAZ. Application fees for operating a mobile phone service in Zimbabwe are also steep, and in 2013, the regulator increased the license fees for mobile networks from US$100 million to $137.5 million. Only one mobile service provider, Econet, had paid this fee in full by end of 2013, while the second largest network, Telecel, had paid a deposit. Zimbabwe has no stringent fees or regulations that hinder the establishment of cybercafes.

While POTRAZ handles the official licensing process for telecoms, insider reports have revealed that the Zimbabwean military may be involved in screening and approving license applications, demonstrating that ICTs are regarded as a security matter for the state. Nevertheless, there have been no reports of harassment or license denials on the basis of political affiliation. Otherwise, internet access prices in Zimbabwe are set by ISPs and cybercafe owners and have thus far been free from state intervention. Individual ISPs submit tariff proposals to POTRAZ, which approves proposals on a case by case basis.

Zimbabwe currently has five international gateways for internet and voice traffic, two of which 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. There are also two trunk switches for the TelOne fixed network and nine mobile switching centers, set up by the country’s three mobile operators. Though private actors are allowed to operate their own gateways, analysts believe they are beholden to a “gentlemen’s agreement” with POTRAZ, which gives the government some level of informal control over the privately-owned telecoms.

19 Zimbabwe Internet Service Providers Association membership list, [http://www.zispa.org.zw/members.html](http://www.zispa.org.zw/members.html).
24 A “trunk switch” is a system that provides network access to many clients by sharing a set of lines or frequencies instead of providing them individually. A “mobile switching center” (MSC) connects calls by switching the digital voice data packets from one network path to another (also called routing). The MSC also provides information that is needed to support mobile service subscribers, such as user registration and authentication information.
Zimbabwe

There have been few cases of deliberate disruptions in connectivity in Zimbabwe, though in the lead-up to the July 2013 general elections, the independent community radio station, Radio Dialogue, reported frequent internet disconnections in its office, and internet cafe owners reported slow internet connectivity.26 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.

ISPs and mobile phone companies are regulated by the telecommunications regulatory body, POTRAZ, whose leaders are appointed by the president in consultation with the minister of transport and communication. POTRAZ has been widely accused of partisanship and politicized decision-making, such as demanding Econet to reconnect Telecel after the former argued that Telecel was operating illegally without paying license fees.27 In August 2013, POTRAZ also intervened in a price war between Econet and Telecel that involved Econet charging 10 cents per minute for its mobile voice service instead of the set tariff of 25 cents. In a move widely seen as an attempt to protect the state-owned network NetOne as well as TeleCel—the latter of which is owned by individuals with links to the ruling party—POTRAZ ordered Econet to revert back to the set tariffs. POTRAZ stated that Econet could not affect a price cut of more than 50 percent without seeking approval. For the first time in many years, Econet publicly complained about POTRAZ's perceived bias, adding that while the other two providers had also slashed prices, no action had been taken against them.28 Another case of political protection of state-owned telecoms players was evidenced in January 2014 when the license fees payment grace period for the state-owned NetOne was extended from June 2014 to 2016, while Econet and Telecel were required to pay the increased license renewal fee of US$137.5 million.29

In late 2013, POTRAZ also attempted to interfere with the operations of Zimfon, a company owned by Zimbabweans based in the United States, after it had launched an unlimited VoIP calling service at a cost of US$13 per month.30 Zimfon planned to sell VoIP lines to Zimbabweans in the diaspora that would operate via an application from Google play or iTunes, while Zimbabweans in the country would connect through mobile phone devices connected on the Africom network. POTRAZ announced, however, that Zimfon’s operations were illegal due to non-compliance with national telecoms regulations,31 though the regulator did not specify which regulations were being violated. POTRAZ’s interference was seen by some as motivated by a concern over potential revenue losses for fixed-line services.

Zimbabwe

Limits on Content

Bulk SMS text messages were blocked during the July 2013 general elections in an apparent effort to restrict opposition campaigning. The government actively tried to silence the anonymous whistleblower using the pseudonym Baba Jukwa, who gained immense popularity and influence on Facebook for his or her daily posts that named and shamed politicians for alleged corruption and informed on the ruling party’s supposed secrets.

In 2013 and early 2014, there were no reports of internet content being blocked or filtered, though in the week leading up to the July 31 elections, the telecommunications regulator POTRAZ issued a directive to the private mobile phone provider, Econet, to block the dissemination of bulk SMS messages sent through its international gateway until after the elections. 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. Meanwhile, ZANU-PF members routinely sent bulk SMS messages via all networks on behalf of President Robert Mugabe’s campaign and other ZANU-PF party candidates.

Though no internet content was blocked during the coverage period, there were numerous indications that the government has the intention to do so. In late November 2013, the online independent news outlet ZimEye reported that ZANU-PF was preparing to ban and block all access to Facebook and other social networking platforms, which are regarded as sources of political subversion. The news stemmed from an anonymous report that was circulated on email networks following reports that a 15 member media delegation from ZANU-PF had recently flown to China for a special exchange program with the Chinese Communist Party (CCP) on methods of controlling the internet. The ZANU-PF Secretary for Information, Rugare Gumbo, denied the allegations, instead stating that the visit to China was intended “primarily to exchange ideas on how to modernize the print and electronic media in so far as information dissemination is concerned.”

In addition, at the party’s annual National People’s Conference in December 2013, ZANU-PF members reportedly urged the government to block foreign-based radio stations, many of which are broadcast over the internet, shortwave frequencies, and satellite. These included London-based Short Wave Radio Africa, Radio Dialogue, Washington DC-based VOA Studio 7, Voice of the People, and Community Radio Harare. According to news reports, the Zimbabwean government has repeatedly jammed the broadcasts from Short Wave Radio Africa since 2005, with equipment and

33 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 SMS,” Newsday, July 26, 2013, https://www.newsday.co.zw/2013/07/26/potraz-bans-bulk-smss/.
training from China,\textsuperscript{37} and has pressured Britain and the United States to shut down the independent radio stations altogether. Apart from this, According to an inside source who attended the December 2013 conference, participants were “taught how to ‘intercept’ broadcasts by the foreign based stations, amongst other things.”\textsuperscript{38}

Suspicion remains that employees of government agencies are restricted in what they can access on the internet while at work. State employees, including those working for state-owned media, exercise self-censorship when sharing politically sensitive information. In the past certain words and names such as “MDC,” and “Morgan Tsvangirai” were blocked at the Central Bank and other government ministries.\textsuperscript{39} This suspicion is bolstered by ZANU-PF’s persistent hostility toward the opposition and independent media, and various ruling party officials often expressed a desire and intent to increase control over ICTs throughout the year.

The pronounced lack of anonymity on social media platforms coupled with the attendant fear of repercussions tends to limit politically oriented statements, since they can be traced back to their authors. Although many journalists contribute to online news platforms, quite a number use pseudonyms when writing about sensitive issues for fear of harassment, and citizens are increasingly using pseudonyms online to discuss political topics.\textsuperscript{40} Debates on the country’s political and socioeconomic issues as well as reactions to online articles about Zimbabwe are mostly confined to chat rooms and feedback sections of online news sites. Concerns over state surveillance have also led to increasing self-censorship, and journalists and human rights defenders who feel threatened often resort to secure email platforms such as Hushmail for correspondence out of concern that the Zimbabwe domain name .co.zw is an open book for state security.

Facebook, Google, Yahoo, and YouTube are among the most popular websites among Zimbabwean internet users. In response to the high unemployment rate, many young people are using social media platforms to solicit business and sell various products. Twitter has been popularized by individual and civil initiatives as a platform to discuss pressing social issues. One such example is the Twitter account @263chat that describes itself as a “start-up media company created to encourage [and] participate in dialogue” and has a following of nearly 32,000 users as of mid-2014.\textsuperscript{41} Media surveys indicate a continuing decline in readership of newspapers coinciding with the rising use of ICT-based platforms for news and other information.\textsuperscript{42} This trend has prompted newspapers to work on integrating online platforms, with nearly all mainstream newspapers now employing online staff and developing strategies for such integration processes.

\textsuperscript{37} “ZANU PF ups anti-pirate radio stations rant,” Zimbabwe Situation, December 17, 2013.
\textsuperscript{38} In its report at the conference ZANU-PF accused the radio stations, which its labels pirate radio stations, of being sponsored by the west to effect regime change as well as “spewing anti-ZANU PF propaganda” to the effect of “distorting people’s national pride.” See, “ZANU PF ups anti-pirate radio stations rant,” Zimbabwe Situation, December 17, 2013.
\textsuperscript{41} @263Chat’s Twitter page: https://twitter.com/263Chat
Independent news websites and other digital media outlets based outside Zimbabwe continue to play a key role as sources of information, especially on sensitive topics that local media groups are afraid of covering. These platforms are used by local journalists and citizens to report on sensitive issues under the cover of pseudonyms. Social media and ICT-based platforms are increasingly being used to mobilize communities around various issues, though growing mobilization efforts have yet to manifest in concrete social, political, or economic change in Zimbabwe.

In March 2013, a self-proclaimed disaffected ZANU-PF member created a Facebook page under the moniker Baba Jukwa, who had drawn a Facebook following of nearly half a million users at its peak. Characterizing himself as a “Concerned father, fighting nepotism and directly linking community with their Leaders, Government, MPs, and Ministers,” Baba Jukwa quickly became a social media sensation for daily posts that named and shamed politicians for alleged corruption and informed on the ruling party’s supposed secrets. Most notably, the anonymous informant was credited with predicting the death of a ZANU-PF member of parliament, Edward Chindori Chininga, who died in a suspicious car accident in June 2013, nine days after Chininga had released a report on widespread corruption in the country’s diamond mines. While the whistleblower’s efforts on Facebook effected little concrete change on the country’s political and social landscape, Baba Jukwa’s popularity was described as representing “the Zimbabwean people’s growing appetite for information and transparency, which will only be fuelled by increasing access to information technology.” Threatened by the Facebook page’s growing influence, Mugabe reportedly offered a US$300,000 reward for Baba Jukwa’s identity in July 2013, and subsequent efforts ultimately led to the unexplained takedown of the anonymous user’s Facebook page in July 2014 (see “Violations of User Rights”).

The 2013 general election became the most internet-fueled election in Zimbabwe’s history, as many social media and information platforms were launched to monitor the electoral process as well as report on electoral fraud. For example, the London-based online news agency, Nehanda Radio, played a key role as a source of information on electoral fraud through its citizen reporting project that allowed citizens to share stories, pictures, and videos on the 2013 elections. Many of the noted electoral irregularities were recorded and shared through platforms such as YouTube, though Robert Mugabe still won the presidency, as expected.

---

Violations of User Rights

A new constitution was adopted in May 2013, providing for press freedom and freedom of expression, though arrests of citizens for their online activities increased during the coverage period, particularly around the period of the general elections in July 2013. One user was arrested for insulting the president on his Facebook page. The anonymous Baba Jukwa Facebook page continued to incite the authorities, leading to aggressive attempts to silence the whistleblower via hacking attacks and other measures. Government surveillance of citizen communications reportedly increased after the July 2013 general elections, and surveillance powers were strengthened with the passage of the Postal and Telecommunications (Subscriber Registration) Regulations in October 2013. The Parliamentary Legal Committee (PLC) declared the new regulations unconstitutional in March 2014, leading to an amended version enacted in July 2014 that provided for judicial oversight but left open a loophole for abuse.

In May 2013, the Zimbabwean parliament approved a new constitution, which the president signed into law shortly thereafter. Sections 61 and 62 of the constitution guarantees freedom of expression, press freedom, access to information, protection for sources of information, and the editorial independence of state-owned media. While these provisions are focused on the traditional media, it is expected that the new rights will extend to the online sphere, which will potentially allow online journalists, bloggers, and social media users to seek protection under the new constitution. Bloggers, however, are not eligible for accreditation as journalists under the Access to Information and Protection of Privacy Act (AIPPA), which provides guidelines for the registration of media organizations and journalist accreditation, as well as punitive measures for violations of these requirements. AIPPA also places restrictions on reporting government information.

The judiciary has sometimes demonstrated a degree of autonomy through rulings that are not favorable to the state, including some freedom of expression cases, though the government often ignores such decisions. An appointment process that allows for high levels of executive interference further compromises judicial independence. No major rulings related to internet freedom occurred during this report’s coverage period.

Meanwhile, 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 the traditional media and online. The CODE punishes 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, though a landmark ruling by the Zimbabwean Constitutional Court in July 2014 declared criminal defamation under the CODE unconstitutional. Nevertheless, Zimbabwe maintains restrictive access to information and media laws, which include the Access to Information and Protection of Privacy Act (AIPPA), the Criminal Codification Act, the Public Order and Security Act, and the Officials Secrets Act, among

Zimbabwe

others. Combined with the extrajudicial actions of both state and non-state actors, these laws severely limit Zimbabweans’ ability to access and share information.

Arrests of citizens for their online activities increased during the coverage period, particularly around the period of the general elections in July 2013. On Election Day, for example, 31-year-old opposition party activist Tonderai Rukato was arrested for posting a photo of a marked ballot displaying a vote for Movement for Democratic Change (MDC) candidate Morgan Tsvangirai on his Facebook page. Charged with contravening the Electoral Act, he was sentenced to ten months in prison, three of which were suspended on condition of good behavior, though he was released in September after serving 31 days in prison when a magistrate ruled in favor of the appeal lodged by MDC lawyers.54 The day after Rukato’s release, however, his family’s local business was set on fire, destroying an estimated US$2,000 worth of goods.

In January 2014, teenage Facebook user Gumisai Manduwa was arrested for allegedly insulting the president after he posted on his Facebook page that President Mugabe “had died and was being preserved in a freezer.”55 Manduwa was released on bail two days after his arrest. His case remains on the court’s docket as of mid-2014.

Meanwhile, the anonymous Facebook user Baba Jukwa continued to incite the ruling party throughout 2013 and 2014, leading President Mugabe to post a US$330,000 reward in July 2013 for any individual willing to unmask the elusive whistleblower.56 Party officials repeatedly tried to have Facebook take down the Baba Jukwa page, the initial failure of which reportedly led the president to seek Chinese technical assistance in censoring the page and identifying its user.57 The Facebook page with a following nearly half a million users was ultimately taken down in July 2014,58 after an editor at the Sunday Mail state newspaper, Edmund Kudakwashe Kudzayi, was arrested in June on accusations of running the Baba Jukwa account.59 His case remains unresolved as of late 2014.

Despite Baba Jukwa’s eventual silencing, political activists inspired by the anonymous Facebook user made phone calls to senior politicians and security chiefs in the lead-up to the general 2013 election, demanding an end to politically motivated violence and a clean election. Unfortunately, the activism resulted in the arrest of Josiah Mahovoya in July 2013 on charges of insulting Police Commissioner General Augustine Chihuri and senior ZANU-PF member Dexter Nduna over the phone. Mahovoya was sentenced to four months in prison, though the nature of the insults was not revealed. He

---

Zimbabwe

reportedly retrieved Chihuri and Nduna’s phone numbers from Baba Jukwa’s Facebook page, and the police had traced the SIM card registration to his name.60

In the meantime, a court case against 21-year old Shantel Rusike is still being dragged through the magistrate courts in Bulawayo as of mid-2014. 61 Rusike was arrested on December 24, 2012 and held for four days after she was reported to the police for sending an image depicting President Mugabe in a nude state via WhatsApp on her mobile phone.62 Rusike faces charges of “causing hatred, contempt or ridicule of the president,” as delineated in the CODE.63

Though the government has proactively endeavored to reveal the identities of certain influential critics on social media sites—such as Baba Jukwa on Facebook—there are no restrictions on users’ ability to communicate anonymously on websites, blogs, or social media platforms. Nonetheless, anonymous communication and 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.64 In August 2013, POTRAZ ordered all unregistered mobile lines to be disconnected in an apparent effort to expand its access to user information for law enforcement purposes.65

On October 1, 2013, the government gazetted a new so-called “spy law” known as the Postal and Telecommunications (Subscriber Registration) Regulations (Statutory Instrument 142/2013), which expanded the scope of subscriber registration requirements previously limited to SIM cards to include “cellular and fixed mobile operators, internet access provider[s] and any other telecommunication licensees or designated agents who provides telecommunication services.”66 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 after either the subscriber or operator has discontinued service. In addition, the regulations require ISPs to provide POTRAZ with copies of their subscriber registers to be stored in a Central Subscriber Information Database to enable POTRAZ to “assist law enforcement agencies on safeguarding national security,” among other aims. 67 Officials could petition POTRAZ for access to the subscriber database without a court order. Following the law’s enactment, the Zimbabwe Internet Services Providers Association released a statement stating that none of its members would participate in email surveillance, though penalties for breaching the new law include both fines and imprisonment.

---


67 Section 8 (1) and (2); https://docs.google.com/file/d/0B0O6T_7m0f19NTR2b18sZjZza2s/edit.
In a positive step in June 2014, the government repealed the legal provisions in the new Subscriber Registration Regulations (Statutory Instrument 142/2013) 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.68 An amended version of the regulations—Statutory Instrument 95/2014—were subsequently enacted in July, which revised section 9(2) to allow law enforcement agents to request information from the central database, “provided that a prior written request is received by the Authority from an official of the law enforcement agency who is in possession of a warrant or court order to obtain such information.”69 Analysis by the Zimbabwean legal watchdog Veritas 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.”70

Government surveillance of citizen communications is also enabled by 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.71 The act also obligates telecoms to report any communications with “offensive” or “threatening” content. Meanwhile, a Monitoring of Interception of Communications Center was established under the Interception of Communications Act of 2007 and has the power to oversee traffic in all telecommunications services and to intercept phone calls, emails, and faxes under the pretext of national security.72 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.73 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,74 and the extent and frequency of monitoring remains unknown.

Suspicions of Chinese technical assistance in controlling ICTs remain strong, particularly following news reports of a ZANU-PF delegation sent to China in November 2013 for a special exchange program on methods of controlling the internet (see “Limits on Content”). In March 2013, the news and internet radio station Nehanda Radio also reported news about a “massive” cyber training

---


program that had begun in 2007 with assistance from Iranian intelligence organizations.\(^\text{75}\) According to the report, personnel from the Zimbabwean armed forces and the Central Intelligence Organization (CIO) have been undergoing intensive cyber training in “technological warfare techniques, counter-intelligence and methods of suppressing popular revolts among others, every six months.” Meanwhile, encrypted communication applications such as Skype remain accessible, though POTRAZ has maintained a September 2011 ban—reportedly enacted for security reasons—on the use of the BlackBerry messenger service that enables users to send free messages.\(^\text{76}\)

In response to fears of civil unrest following ZANU-PF’s overwhelming victory in the July 2013 general elections, the ruling party via the CIO reportedly ramped up its mass monitoring and interception efforts. According to an inside source within the security forces, “targeted groups and individuals’ communication and social media activities are being monitored, and at times the CIO obtains recordings of voice calls from local cellphone providers under the guise of carrying out state security operations.”\(^\text{77}\) One incident involving the interception and publication of emails belonging to Elizabeth Macheka, the wife of MDC leader and former Prime Minister Morgan Tsvangirai, illuminates the extent to which ZANU-PF abuses surveillance for political purposes. In August 2013, the front page of the state-owned Sunday Mail published a story alleging that Macheka was having an affair with a former lover.\(^\text{78}\) The story was based on supposed email exchanges between Macheka and the alleged boyfriend, which were quoted extensively throughout the article. While Macheka never confirmed the authenticity of the emails, the MDC party dismissed the story as an attempt to distract the country from what they regarded as a stolen election.

Opposition political groups also reportedly monitor the social media activities of their members. While caught up in intraparty fighting in March 2014, the opposition party MDC-T, an offshoot of the MDC, stated that it monitors the activities of the party leaders on Facebook. MDC-T spokesperson Douglas Mwonzora said that the move was aimed at members who post hate speech, though the opposition party is reported to have used some Facebook posts as evidence of insubordination in suspending senior officials in the past.\(^\text{79}\)

Extralegal harassment, attacks, and intimidation against media workers in the print, radio, and broadcast sectors is common in Zimbabwe, and as news outlets have increased their influence in the online sphere, attacks against online outlets have increased in tandem. One incident in April 2014 involved Bulawayo-based aspiring community radio station Radio Dialogue, which was raided by the police and POTRAZ officers who confiscated internet service payment receipts, reportedly to trace

---

76 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,” The Zimbabwean, June 5, 2012, http://www.thezimbabwean.co.uk/technology/58636/blackberry-messenger-a-dream.html.
Radio Dialogue’s online activities. Technical attacks against critical websites and social media pages are also increasing. Most notably in 2013 and 2014, the authorities launched several hacking attacks against the anonymous whistleblower Baba Jukwa’s Facebook page, resulting in the deletion of some of Jukwa’s damaging posts in 2013 and its ultimate takedown in July 2014.

---


Methodology

*Freedom on the Net* provides analytical reports and numerical ratings for 65 countries worldwide. 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 May 1, 2013 and May 31, 2014.

**What We Measure**

The *Freedom on the Net* index aims to measure each country’s level of internet and digital media freedom based on a set of methodology questions described below (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 index aims to capture the entire “enabling environment” for internet freedom within each country through a set of 21 methodology questions, divided into three subcategories, which are intended to highlight the vast array of relevant issues. Each individual question is scored on a varying range of points. Assigning numerical points allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. Countries are given a total score from 0 (best) to 100 (worst) as well as a score for each sub-category. Countries scoring between 0 to 30 points overall are regarded as having a “Free” internet and digital media environment; 31 to 60, “Partly Free”; and 61 to 100, “Not Free”. An accompanying country report provides narrative detail on the points covered by the methodology questions.

The methodology examines the level of internet freedom through a set of 21 questions and nearly 100 accompanying subpoints, organized into three groupings:

- **Obstacles to Access**—including infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; legal and ownership control over internet and mobile phone access providers.
- **Limits on Content**—including 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.
- **Violations of User Rights**—including legal protections and restrictions on online activity; surveillance and limits on privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

The purpose of the subpoints is to guide analysts regarding factors they should consider while evaluating and assigning the score for each methodology question. After researchers submitted their draft scores, 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 the 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.
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.
- 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.
- Unless otherwise indicated, the sub-questions listed are meant to provide guidance as to what issues should be addressed under each methodology question, though not all will apply to every country.

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?

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 socio-economic 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)
   - Does the government place limits on the amount of bandwidth that access providers can supply?
• Does the government use control over internet infrastructure (routers, switches, etc.) to limit connectivity, permanently or during specific events?
• Does the government centralize telecommunications infrastructure in a manner that could facilitate control of content and surveillance?
• Does the government block protocols and tools that allow for instant, person-to-person communication (VOIP, instant messaging, text messaging, etc.), particularly those based outside the country (e.g. Skype, WhatsApp, etc.)?
• Does the government block protocols, social media, and/or communication apps that allow for information sharing or building online communities (video-sharing, social-networking sites, comment features, blogging platforms, etc.) permanently or during specific events?
• Is there blocking of certain tools that enable circumvention of online filters and censors?

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 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 does the government 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 the government 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 directives 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-costs 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)

• 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?

http://www.freedomhouse.org
• 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, including via deep-packet inspection?
• 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 providers 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, Program Officer and Research Analyst (Africa), Freedom on the Net
Madeline Earp, Research Analyst (Asia), Freedom on the Net
Laura Reed, Research Analyst (Eurasia & EU), Freedom on the Net
Adrian Shahbaz, Research Analyst (MENA & EU), Freedom on the Net
Ashley Greco-Stoner, Senior Research Assistant (Latin America), Freedom on the Net

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, Research Assistant, CELE

Armenia: Seda Muradyan, Co-Founder, Public Journalism Club NGO, and Armenia Branch Country Director, Institute for War and Peace Reporting

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 Geybullayeva, freelance blogger and journalist

Bangladesh: Dr. Faheem Hussain, Assistant Professor, Department of Technology and Society, State University of New York (SUNY) Korea

Brazil: Carolina Rossini, Vice President, International Policy, at Public Knowledge; Fabrício Bertini Pasquot Polido, Professor, Law School of Federal University of Minas Gerais, and Head of Center for International Studies on Internet, Innovation and Intellectual Property – GNet

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, University of Ottawa

China: Madeline Earp, Research Analyst, Freedom on the Net, Freedom House

Colombia: Carlos Cortés, Media Policy Consultant, and Researcher of the Center for Freedom of Expression Studies (CELE) at Palermo University, Argentina

Cuba: Ernesto Hernández Busto, Cuban journalist and writer, Barcelona

Estonia: Linnar Viik, Lecturer, Board Member, Estonian IT College

France: Jean-Loup Richet, Researcher, University of Nantes

Georgia: Teona Turashvili, Analyst at Institute for Development of Freedom of Information (IDFI), Georgia

Germany: Philipp Otto, Digital Strategist and Editor in Chief, iRights.info, Founder, iRights.Lab think tank, iRights.Media publishing house; Henning Lahmann, Research Assistant, iRights.Lab.

Hungary: Borbála Tóth, Independent Researcher

Iceland: Caroline Nellemann, Independent Consultant and Specialist in Digital Media and Civic Engagement
India: Chinmayi Arun, Research Director, Center for Communication Governance at National Law University, Delhi, Sarvejot Singh, Project Manager and Research Fellow, Centre for Communication Governance. Parul Sharma, Student, B.A., LL.B. (Hons.), National Law University, Medha Vikram, Student, B.A., LL.B. (Hons.), National Law University.

Indonesia: Indriaswati Dyah Saptaningrum, Executive Director, ELSAM (The Institute for Policy Research and Advocacy)

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: Abeer al-Najjar, Assistant Professor of Journalism and Media Studies, American University of Sharjah

Kazakhstan: Adil Nurmakov, Senior Lecturer, KIMEP University

Kenya: Grace Githaiga, Associate, Kenya ICT Action Network (KICTANet)

Kyrgyzstan: Artem Goriyanov, IT Programs Director, Public Foundation CIIP

Lebanon: Dr. Jad Melki, Assistant Professor of Journalism and Media Studies and Director, Media Studies Program, American University of Beirut

Libya: Danya Bashir Hobba, Ambassador, One Young World

Malawi: Gregory Gondwe, Bureau Chief, Times Media Group, Malawi

Malaysia: K. Kabilan, Managing Editor, The Ant Daily

Mexico: Jorge Luis Sierra, Director, Knight International Journalism Fellowships, International Center for Journalists

Morocco: Bouziane Zaid, Assistant Professor of Media and Communication, Al Akhawayn University in Ifrane

Myanmar: Min Zin, PhD Candidate, Department of Political Science, University of California, Berkeley, and Contributor, Foreign Policy Democracy Lab channel

Nigeria: 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria

Pakistan: Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan, Lawyer and Internet Freedom Activist

Philippines: Jacques D.M. Gimeno, Assistant Professor, Communication Research Department, University of the Philippines-Diliman

Saudi Arabia: Abeer Allam, former Riyadh-based Correspondent, Financial Times

Singapore: Cherian George, Associate Professor, School of Communication, Hong Kong Baptist University

South Africa: Alan Finlay, Independent Consultant, Open Research

South Korea: Dr. Yenn Lee, Research Skills Trainer/Coordinator, School of Oriental and African Studies, University of London

Sri Lanka: Nigel V. Nwawela, Independent writer and researcher

Syria: Dlshad Othman, ICT Specialist, Information Safety & Capacity Project (ISC)

Turkey: Yaman Akdeniz, Professor of Law, Istanbul Bilgi University and Founder of Cyber-Rights.org

Uganda: Lillian Nalwoga, Policy Officer, Collaboration on International ICT Policy in East and Southern Africa (CIPESA), President, Internet Society Uganda Chapter

Ukraine: Tetyana Lokot, Doctoral Student and Researcher, Philip Merrill College of Journalism, University of Maryland, College Park and Coeditor, RuNet Echo at Global Voices

United Kingdom: LSE Media Policy Project, London School of Economics and Political Science

United States: Emily Barabas, Policy Analyst, Center for Democracy and Technology

Uzbekistan: Zhanna Hördegen, Independent Consultant and Research Associate at the University Research Priority Program Asia and Europe, University of Zurich

Venezuela: Raisa Urribarri, Director, Communications Lab for Teaching, Research and Community Extension (LIESR) at the University of Los Andes.

Zambia: Brenda Nglazi Zulu, Founder and Director, Africa Interactive Media and Zambian Bloggers Network

The analysts for the reports on Angola, Bahrain, Belarus, Ecuador, Egypt, Ethiopia, The Gambia, Russia, Rwanda, Thailand, Tunisia, Sudan, United Arab Emirates, Vietnam and Zimbabwe are independent internet researchers who have requested to remain anonymous. Xiao Qiang, founder and chief editor of China Digital Times, and adjunct professor of the School of Information, University of California at Berkeley, was an advisor for the China report.
The internet is a crucial medium not just for personal communication or news and information, but for political participation and civic engagement. The struggle for internet freedom is consequently inseparable from the struggle for freedom of every kind.