EVOLVING TACTICS OF INTERNET CONTROL AND THE PUSH FOR GREATER FREEDOM

By Sanja Kelly and Sarah Cook

As of 2012, nearly a third of the world's population has used the internet, and an even greater portion possesses a mobile phone. The internet has transformed the way in which people obtain news, conduct business, communicate with one another, socialize, and interact with public officials. Concerned with the power of new technologies to catalyze political change, many authoritarian states have taken various measures to filter, monitor, or otherwise obstruct free speech online. These tactics were particularly evident over the past year in countries such as Saudi Arabia, Ethiopia, Uzbekistan, and China, where the authorities imposed further restrictions following the political uprisings in Egypt and Tunisia, in which social media played a key role.

To illuminate the nature of these evolving threats and identify areas of growing opportunity, Freedom House has conducted a comprehensive study of internet freedom in 47 countries around the globe. This report is the third in its series and focuses on developments that occurred between January 2011 and May 2012. The previous edition, covering 37 countries, was published in April 2011. *Freedom on the Net 2012* assesses a greater variety of political systems than its predecessors, while tracing improvements and declines in the countries examined in the previous two editions. Over 50 researchers, nearly all based in the countries they analyzed, contributed to the project by researching laws and practices relevant to the internet, testing the accessibility of select websites, and interviewing a wide range of sources.

This year's findings indicate that restrictions on internet freedom in many countries have continued to grow, though the methods of control are slowly evolving and becoming less visible. Of the 47 countries examined, 20 have experienced a negative trajectory since January 2011, with Bahrain, Pakistan, and Ethiopia registering the greatest declines. In Bahrain, Egypt, and Jordan, the downgrades reflected intensified censorship, arrests, and violence against bloggers as the authorities sought to quell public calls for political and economic reform. Declines in Mexico occurred in the context of increasing threats of violence from organized crime, which began to directly influence free speech online. Ethiopia presented an unusual dynamic of growing restrictions in a country with a tiny population of users, possibly reflecting a government effort to establish more sophisticated controls before allowing access to expand. And Pakistan's downgrade reflected extreme punishments meted out for dissemination of allegedly blasphemous messages and the increasingly aggressive efforts of the telecom regulator to censor content transmitted via information and communications technologies (ICTs).

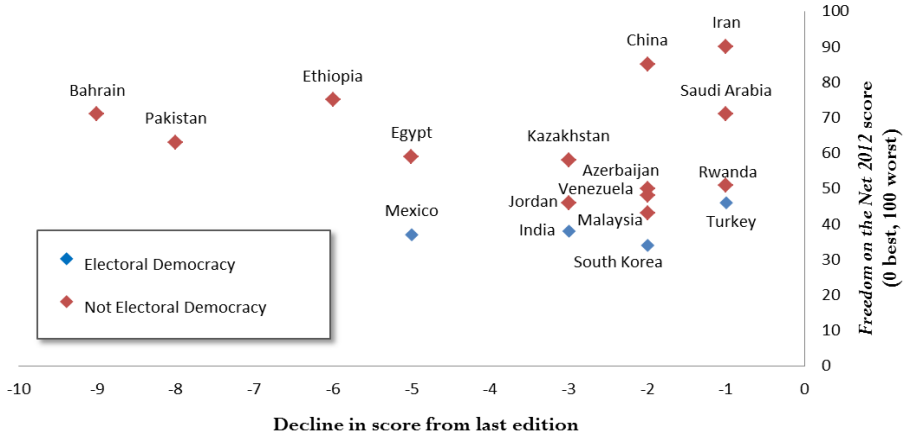
Sanja Kelly is the project director for *Freedom on the Net* at Freedom House. **Sarah Cook** is a senior research analyst at Freedom House.

At the same time, 14 countries registered a positive trajectory. In some countries—such as Tunisia, Libya, and Burma—this was the result of a dramatic regime change or political opening. Elsewhere—as in Georgia, Kenya, and Indonesia—the improvements reflected a growing diversity of content and fewer cases of arrest or censorship than in previous years. The remaining gains occurred almost exclusively in established democracies, highlighting the crucial importance of broader institutions of democratic governance—such as elected representatives, free civil society, and independent courts—in upholding internet freedom. While proposals that could negatively affect internet freedom did emerge in democratic states, civil society, the media, and the private sector were more likely to organize successful campaigns to prevent such proposals from being formally adopted, and the courts were more likely to reverse them. Only 4 of the 20 countries that recently experienced declines are considered electoral democracies (see figure below).

Despite the noted improvements, restrictions on internet freedom continue to expand across a wide range of countries. Over the past decade, governments have developed a number of effective tools to control the internet. These include limiting connectivity and infrastructure, blocking and filtering content that is critical of the regime, and arresting users who post information that is deemed undesirable. In 2011 and 2012, certain methods that were previously employed only in the most oppressive environments became more widely utilized.

To counter the growing influence of independent voices online, an increasing number of states are turning to proactive manipulation of web content, rendering it more challenging for regular users to distinguish between credible information and government propaganda. Regimes are covertly hiring armies of pro-government bloggers to tout the official point of view, discredit opposition activists, or disseminate false information about unfolding events. This practice was in the past largely limited to China and Russia, but over the last year, it has been adopted in more than a quarter of the countries examined. The Bahraini authorities, for example, have employed hundreds of "trolls" whose responsibility is to scout popular domestic and international websites, and while posing as ordinary users, attack the credibility of those who post information that reflects poorly on the government.

INTERNET FREEDOM AND DEMOCRACY



Of the 17 countries that experienced numerical declines since the 2011 edition of *Freedom on the Net,* only four are designated as electoral democracies by Freedom House's flagship publication *Freedom in the World.* Another three countries included for the first time in *Freedom on the Net 2012* showed a negative trajectory since January 2011: Sri Lanka, Syria, and Uzbekistan. None of the three are electoral democracies.

Both physical and technical attacks against online journalists, bloggers, and certain internet users have also been on the rise in 2011 and 2012, demonstrating that the tactics previously used against opposition journalists are now being applied to those writing in the online sphere as well. Moreover, the attacks have become more violent. In Azerbaijan, for example, a prominent journalist and contributor to several online news sites died of stab wounds after being attacked by unknown assailants. In Mexico, for the first time, individuals who had circulated information online about organized crime and corruption were brutally murdered, with the killers often leaving notes that cited the victim's online activities.

As another method of controlling speech and activism online, governments have imposed temporary shutdowns of the internet or mobile phone networks during mass protests, political events, or other sensitive times. While the most widely reported example occurred in Egypt in January 2011, this report's findings reveal that both nationwide and localized shutdowns are becoming more common. Prior to its downfall, the Qadhafi regime in Libya shut off the internet nationwide in March 2011, and large swaths of the country remained disconnected until August 2011. Select regions in Syria have experienced repeated internet shutdowns during 2011 and 2012, as the regime has tried to prevent citizens from spreading information and videos about the government's attacks on civilians. Localized internet shutdowns also occurred in China and Bahrain during antigovernment protests, and localized mobile phone shutdowns occurred in India and Pakistan due to security concerns.

Based on the types of controls implemented, many of the countries examined in this edition of *Freedom on the Net* can be divided into three categories:

1. **Blockers:** In this set of countries, the government has decided to block a large number of politically relevant websites, often imposing complete blocks on certain social-media platforms. The state has also invested significant resources in technical capacity and manpower to identify content for blocking. Among the countries that fall into this category are Bahrain, China, Ethiopia, Iran, Saudi Arabia, Vietnam, Syria, Thailand, and Uzbekistan. Although most of these governments employ a range of other tactics to curb internet freedom—including imposing pressure on bloggers and internet service providers, hiring pro-government commentators, and arresting users who post comments that are critical of the authorities—they use blocking and filtering as a key tool for limiting free expression. Over the past year, governments in this group have continued to refine their censorship apparatus and devoted greater energy to frustrating user attempts to circumvent the official blocking.

2. **Nonblockers:** In this category, the government has not yet started to systematically block politically relevant websites, though the authorities may have demonstrated interest in restricting online content, particularly after witnessing the role online tools can play in upending the political status quo. Most often, these governments seek the appearance that their country has a free internet, and prefer to employ less visible or less traceable censorship tactics, such as behind-the-scenes pressure from government agents to delete content, or anonymous cyberattacks against influential news sites at politically opportune times. These states also tend

to have a harsh legal framework surrounding free speech, and in recent years have arrested individuals who posted online information that is critical of the government. Among the countries that fall into this category are Azerbaijan, Egypt, Jordan, Malaysia, Venezuela, and Zimbabwe.

3. **Nascent blockers:** These countries—including Belarus, Sri Lanka, Pakistan, and Russia—appear to be at a crossroads. They have started imposing politically motivated blocks, but the system has not yet been institutionalized, and it is often sporadic. For example, in Russia, the government officially blocks material deemed to promote "extremism," but due to the vague definition of extremism, political websites are occasionally blocked as well. In addition, regional courts in Russia have at times ordered the blocking of websites that unveil local corruption or challenge local authorities. Other countries in this group, such as Pakistan, have seriously considered instituting nationwide filtering, but have not yet implemented it, thus not fully crossing into the first category.

Despite the growing threats, the study's findings reveal a significant uptick in citizen activism related to internet freedom, which has produced several notable mobilization efforts and legislative victories. In several European countries, fierce public opposition to the Anti-Counterfeiting Trade Agreement (ACTA) has prompted governments to step away from ratification of the treaty. In Pakistan, nongovernmental organizations (NGOs) and activists played a key role in exposing and resisting the government's plan to impose systematic, nationwide filtering. In Turkey, demonstrations against a proposal to implement mandatory filtering of content deemed "harmful" to children and other citizens drew as many as 50,000 people, prompting the government to back down and render the system voluntary. In the United States, campaigns by civil society and technology companies helped to halt passage of the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA), which were criticized for their potentially negative effects on free speech. The simultaneous blacking out of popular websites by their administrators as a form of protest helped increase public awareness of the two bills, and the tactic has since been repeated in countries like Jordan and Italy in the face of potentially restrictive legislation.

In largely democratic settings, the courts have started to play an instrumental role in defending internet freedom and overturning laws that may infringe on it. In Hungary, the Constitutional Court decided in December 2011 that the country's restrictive new media regulations would not be applicable to online news sources and portals. In South Korea in August 2012, the Constitutional Court issued its third decision favorable to internet freedom in two years, ruling against the real-name registration system. In countries where the judiciary is not independent, public and international pressure ultimately yielded executive branch decisions that nullified negative court rulings. In Azerbaijan, Bahrain, China, Egypt, Syria, Russia, and Saudi Arabia, at least one jailed blogger or internet activist was pardoned or released from extralegal detention following a high-profile campaign on his or her behalf. And in a dramatic reversal from previous practice, dozens of activists were released from prison in Burma, though the restrictive laws under which they had been jailed remained in place.

Since 2011, China has exerted a greater influence in the online world, emerging as an incubator for sophisticated new types of internet restrictions. The Chinese method for controlling social-media content—restricting access to international networks while coercing their domestic alternatives to robustly censor and monitor user communications according to Communist Party directives—has become a particularly potent model for other authoritarian countries. Belarus's autocratic president has praised China's internet controls, and Uzbekistan has introduced several social-media platforms on which users must register with their real names and administrators have preemptively deleted politically sensitive posts. In Iran, a prominent internet specialist likened the intended outcome of the country's proposed National Internet scheme to the Chinese censorship model, with users enjoying "expansive local connections," but having their foreign communications filtered through a "controllable channel." Meanwhile, reports have emerged of Chinese experts, telecommunications companies, or hackers assisting the governments of Ethiopia, Libya, Sri Lanka, Iran, and Zimbabwe with attempts to enhance their technical capacity to censor, monitor, or carry out cyberattacks against regime opponents.

Alongside China, authoritarian countries such as Russia, Tajikistan, and Uzbekistan have recently increased efforts on the international stage to institutionalize some of the restrictions they already implement within their own borders. For example, this coalition of states in 2011 submitted to the United Nations General Assembly a proposal for an internet "code of conduct," which would, among other things, legitimize censoring of any website that "undermines political and social order." Moreover, some of these countries have been at the forefront of an effort to expand the mandate of the International Telecommunication Union—a UN agency—to include certain internet-related matters, which could negatively impact free expression, user privacy, and access to information.

KEY TRENDS

Freedom on the Net 2012 identifies a shifting set of tactics used by various governments to control the free flow of information online. While blocking and filtering remain the preferred methods of restriction in many of the states examined, a growing set of countries have chosen other tools to limit political and social speech that they view as undesirable. These alternative tactics include (1) introduction of vague laws that prohibit certain types of content, (2) proactive manipulation, (3) physical attacks against bloggers and other internet users, and (4) politically motivated surveillance.

New Laws Restrict Free Speech and Prompt Arrests of Internet Users

Responding to the rise of user-generated content, governments around the world are introducing new laws that regulate online speech and prescribe penalties for those found to be in violation of the established rules. The threat in many countries comes from laws that are ostensibly designed to protect national security or citizens from cybercrime, but which are so broadly worded that they can easily be turned on political opponents. In Ethiopia, for example, a prominent dissident blogger

was recently sentenced under an antiterrorism law to 18 years in prison for publishing an online article that called for greater political freedom. In Egypt, after the fall of President Hosni Mubarak in early 2011, several bloggers were detained and sentenced to prison for posts that were critical of the military or called for protests against military rule.

Countries that passed a new law in 2011-2012 that negatively impacts internet freedom: *Argentina, Bahrain, Belarus, Burma, China, India, Indonesia, Iran, Kazakhstan, Kyrgyzstan, Malaysia, Mexico, Pakistan, Russia, Saudi Arabia, Sri Lanka, Syria, Thailand, Vietnam*

Of the 47 countries analyzed in this edition, 19 have passed new laws or other directives since January 2011 that could negatively affect free speech online, violate users' privacy, or punish individuals who post certain types of content. In Saudi Arabia, a new law for online media, which took effect in February 2011, requires all news websites and websites that host video or audio content to register with the government. Similarly, the government of Sri Lanka issued a directive that requires websites "carrying any content relating to Sri Lanka" to register for accreditation with the Ministry of Mass Media and Information, whether they are based inside or outside the country. While the authorities often claim that such regulations will "protect" online journalists or users, in effect they make it easier to block and fine websites containing content that is politically or socially unacceptable to the government.

An increasing number of countries are passing laws or interpreting current legislation so as to make internet intermediaries legally liable for the content posted through their services. For instance, in April 2012, Malaysia's parliament passed an amendment to the 1950 Evidence Act that holds the hosts of online forums, news outlets, blogging services, and businesses providing WiFi responsible for any seditious content posted by anonymous users. In Thailand, pressure on intermediaries intensified in May 2012 after a forum moderator for the popular online news outlet *Prachatai* received a suspended eight-month jail sentence and a fine for not deleting quickly enough an anonymous reader's criticism of the royal family.

As a consequence, intermediaries in some countries are voluntarily taking down or deleting potentially offending websites or posts on social networks to avoid legal liability. In the most extreme example, intermediary liability in China has resulted in private companies maintaining whole divisions responsible for monitoring the content of blogs, microblogs, search engines, and online forums, deleting tens of millions of messages or search results a year based on administrators' interpretation of both long-standing taboos and daily Communist Party directives. Reports have emerged of similar preemptive deletion by moderators in other countries, such as Kazakhstan, Vietnam, and Saudi Arabia.

In India, amid several court cases regarding intermediaries' responsibility for hosting illegal content and new guidelines requiring intermediaries to remove objectionable content within 36 hours of notice, much evidence has surfaced that intermediaries are taking down content without fully evaluating or challenging the legality of the request. For example, in December 2011, the website "Cartoons against Corruption" was suspended by its hosting company after a complaint filed with

the Mumbai police alleged that the site's cartoons ridiculed India's parliament and national emblems. As a result of such dynamics, large swaths of online content are disappearing, and the losses are far more difficult to reverse than the mere blocking of a website.

Laws that restrict free speech are also forcing a growing number of internet users and content providers into court, or putting them behind bars. Two Tunisians were given seven-year prison sentences in March 2012 for publishing online content that was perceived as offensive to Islam and "liable to cause harm to public order or public morals," an offense found in the largely unreformed penal code from the era of autocratic former president Zine el-Abidine Ben Ali. In some countries, harsh penalties are also applicable to content transmitted through other ICTs as evidenced in the case of a Pakistani man who was sentenced to death in 2011 for sending an allegedly blasphemous text message via his mobile phone. In Thailand, a 61-year-old man was sentenced to 20 years in prison after he allegedly sent four mobile phone text messages that were deemed to have insulted the monarchy; several months into his sentence he died in prison due to illness.

In 26 of the 47 countries assessed, a blogger or other ICT user was arrested for content posted online or sent via mobile phone text message.

Paid Commentators, Hijacking Attacks Spread Misinformation

In addition to taking steps to remove unfavorable content from the internet, a growing number of governments are investing significant resources and using deceptive tactics to manipulate online discussions. Already evident in a small sets of countries assessed in previous editions of *Freedom on the Net*, the phenomenon of paid pro-government commentators has spread over the past two years, appearing in 14 of the 47 countries examined in this study. Even where such dynamics had previously emerged, their prevalence has evolved and expanded, as governments seek to undermine public trust in independent sources of information and counter the influence of particular websites and activists.

Countries where pro-government commentators were used to manipulate internet discussions in 2011-2012: *Bahrain, Belarus, China, Cuba, Egypt, Ethiopia, Iran, Malaysia, Russia, Saudi Arabia, Syria, Thailand, Ukraine, Venezuela*

Paid commentators rarely reveal their official links when posting online, nor do governments inform taxpayers that state funds are being spent on such projects. Moreover, some of the tactics used to manipulate online discussions—including spreading false statements or hacking into citizens' accounts—are illegal in many of the countries where they occur. In Cuba, an estimated 1,000 bloggers recruited by the government have disseminated damaging rumors about the personal lives of the island's influential independent bloggers.

In some countries, such as Bahrain and Malaysia, the government or ruling party is reported to have hired international public relations firms to engage in such activities on its behalf. In Russia, media reports indicated that the ruling party planned to invest nearly $320,000 to discredit prominent

blogger Aleksey Navalny, including through a possible scheme to disseminate compromising videos using a Navalny look-alike. China's paid pro-government commentators, known informally as the "50 Cent Party," are estimated to number in the hundreds of thousands, while an Iranian official claimed in mid-2011 that 40 companies had received over $56 million to produce pro-government digital content.

Rather than creating their own websites or social-media accounts to influence online discussion, some governments or their supporters have hijacked the online presence of their critics and altered the content posted in an effort to deceive the growing audience of citizens who are shifting from state-controlled media to alternative sources of news. In Jordan, the popular *Amman News* website was hacked, and a sensitive statement by tribal leaders calling for reforms was forcibly deleted. In Burma, prior to the government's shift to a more tolerant attitude toward dissent, the website of the exile news outlet *Irrawaddy* was hacked, and fake news items that could discredit the outlet or sow discord among the opposition were posted. In Egypt, in the run-up to elections in late 2011 and early 2012, a Facebook account used for reporting electoral violations was hacked, and pro-military messages were disseminated.

***Countries where government critics faced politically motivated cyberattacks in 2011-2012**: Bahrain, Belarus, Burma, China, Egypt, Iran, Jordan, Kazakhstan, Libya, Malaysia, Mexico, Russia, Saudi Arabia, Syria, Thailand, Uzbekistan, Venezuela, Vietnam, Zimbabwe*

Some hijackings or impersonations have targeted influential individuals rather than news websites. In early 2012, a fake Twitter account was created using the name of a British-Syrian activist whose reports on a massacre by Syrian government forces had drawn international attention. The fake account's postings combined plausible criticism of the regime with comments that seemed to incite sectarian hatred. In one of the most notable examples of this dynamic, since August 2011, the blogs and Twitter accounts of at least two dozen government critics and prominent figures in Venezuela—including journalists, economists, artists, and writers—have been hacked and hijacked. The messages disseminated in their names have ranged from support for the government's economic policy and criticism of the opposition presidential candidate to threatening comments directed at other users.

Physical Attacks against Government Critics Intensify

Governments and other powerful actors are increasingly resorting to physical violence to punish those who post critical content online, with sometimes fatal consequences. In 19 of the 47 countries assessed, a blogger or internet user was tortured, disappeared, beaten, or brutally assaulted. In five countries, an activist or citizen journalist was killed in retribution for information posted online that exposed human rights abuses.

This rise in violence has taken different forms in different countries. In some repressive states—like China, Iran, Saudi Arabia, Syria, and Vietnam—reports abound of individuals being tortured in

custody after being detained for online activities. In Bahrain, the moderator of an online forum was killed in police custody in April 2011, within one week of his arrest. His body showed clear signs of abuse, and a commission of inquiry subsequently confirmed his death under torture. In other countries, such as Cuba, the authorities have shifted tactics, replacing long-term imprisonment with extralegal detentions, intimidation, and occasional beatings. In Sri Lanka and Uzbekistan, online critics of the government have disappeared under mysterious circumstances, with previous official harassment fueling suspicions that they are being illegally detained.

In China, following online calls for a Tunisian-style Jasmine Revolution in February 2011, dozens of bloggers, lawyers, and activists who had large followings on social-media sites were abducted in one of the worst crackdowns on free expression in recent memory. Several of those detained were sentenced to long prison terms, but most were released after weeks of incommunicado detention, with no legal record or justification for their arrest. Many reported being beaten, deprived of sleep, or otherwise abused, with at least one lawyer contracting tuberculosis within only 21 days in custody.

Countries where a blogger or ICT user was physically attacked or killed in 2011-2012: *Azerbaijan, Bahrain, Burma, China, Cuba, Egypt, Indonesia, Iran, Jordan, Kazakhstan, Libya, Mexico, Pakistan, Saudi Arabia, Sri Lanka, Syria, Thailand, Uzbekistan, Vietnam*

In a newly emerging phenomenon, bloggers and citizen journalists in a number of countries were specifically targeted by security forces while reporting from the field during periods of unrest or armed conflict. In Kazakhstan, a blogger was reportedly assaulted by police who held a pistol to his head after he uploaded video footage to YouTube that showed local residents protesting a government crackdown. In Egypt, several well-known online activists were badly injured during police and military assaults on protesters, causing one blogger to lose his right eye and another to suffer 117 birdshot wounds. The circumstances surrounding the attacks raised suspicions that the individuals had been singled out by members of the security forces, who either responded to their filming of events or recognized them as influential online opinion leaders. In both Libya and Syria, citizen journalists who had gained international prominence for their live online video broadcasts were killed in targeted attacks by government forces.

Bloggers and citizen journalists are also facing violence by nonstate actors or unidentified attackers. But even in these cases, impunity for the perpetrators or possible pro-government motives have given the assaults an appearance of at least tacit official approval. In Indonesia, Islamists beat a man who had started a Facebook group promoting atheism, then reported him to the authorities. Police arrived and arrested the user, who was subsequently prosecuted, while the attackers went unpunished. In Thailand, a professor leading a petition campaign to amend restrictive lèse-majesté legislation was assaulted by two unidentified people in an incident that rights groups believed was connected to his advocacy. In some countries, attacks by nonstate actors have proved fatal, as with the killings in Mexico mentioned above. In Pakistan, a series of bombing attacks against cybercafes by Islamist militants have led to several deaths and dozens of injuries.

Some of these attacks against online writers are especially cruel. In Jordan, a female blogger was stabbed in the stomach. In Kazakhstan, reporters from an online television station were beaten with baseball bats. In Egypt, an online columnist suffered broken wrists after being beaten and sexually assaulted. In Syria, the body of a freelance photographer killed by security forces was mutilated. And in China and Uzbekistan, detained activists and journalists were forcibly medicated with psychiatric drugs.

However, extralegal harassment of online activists and bloggers is not always so extreme. In a wide range of countries, intimidation takes more mundane but also more pervasive forms. In Bahrain, Belarus, Cuba, Turkey, Thailand, and Vietnam, individuals have been fired from their jobs, barred from universities, or banned from traveling abroad after posting comments that criticize the government or otherwise cross "red lines." In Russia and Azerbaijan, the harassment has expanded to activists' families, with parents receiving calls from security personnel who press them to stop their adult children's activism.

In addition to individual users, the offices of news websites or free expression groups have been subject to arbitrary attacks. In Belarus, Jordan, and Thailand, security forces or unidentified armed men raided the editorial offices of popular online news and information sites, confiscating or destroying equipment. In Venezuela, the offices of a civil society group that is active in defending online freedom of expression were burglarized on two occasions. And in Sri Lanka, an arson attack destroyed the offices of a popular online news site that had supported the president's competitor in the 2010 election.

Surveillance Increases, with Few Checks on Abuse

Many governments are seeking less visible means to infringe upon internet freedom, often by increasing their technical capacity or administrative authority to access private correspondence via ICTs. Governments across the full spectrum of democratic performance—including South Korea, Kenya, Thailand, Egypt, and Syria—have enhanced their surveillance abilities in recent years or announced that they intend to do so. Of the 19 countries that passed new regulations negatively affecting internet freedom in 2011 and early 2012, 12 disproportionately enhanced surveillance or restricted user anonymity. Although some interception of communications may be necessary for fighting crime or preventing terrorist attacks, surveillance powers are abused for political ends in many countries. Even in democratic settings, proper procedures are not always followed, resulting in violations of user privacy.

In the more repressive and technically sophisticated environments, authorities engage in bulk monitoring of information flows, often through a centralized point. Intelligence agencies then gain direct access to users' communications across a range of platforms—mobile phone conversations, text messages, e-mail, browsing history, Voice over IP discussions, instant messaging, and others. The most advanced systems scan the traffic in real time, with preset keywords, e-mail addresses, and phone numbers used to detect communications of interest to the authorities. Voice-recognition

software is being applied in a growing number of countries to scan spoken conversations for either sensitive keywords or particular individuals' voices. Even in less technologically advanced settings, the government has little trouble accessing user communications once an offender has been identified, as service providers can be required to retain data and content and submit them to the authorities upon request. In most authoritarian countries, security services can intercept communications or obtain user data from service providers without a judicial warrant. Some democratic governments also have highly advanced monitoring equipment, but court approval is needed to access user information, and what is retained usually involves the time and recipients of communications rather than their actual content.

Surveillance in nondemocratic countries is often political in nature, aimed at identifying and suppressing government critics and human rights activists. Such monitoring can have dire repercussions for the targeted individuals, including imprisonment, torture, and even death. In Belarus, Bahrain, Ethiopia, and elsewhere, activists found that their e-mails, text messages, or Skype communications were presented to them during interrogations or used as evidence in politicized trials. In Libya, following Mu'ammar al-Qadhafi's ouster, journalists discovered a sophisticated monitoring center and a storage room filled with dossiers of the online activities of both Libyans and foreigners. Such revelations have raised serious ethical questions and public relations problems for Chinese companies and some firms based in developed democracies that have been known to supply surveillance tools to repressive regimes.

Even governments with sophisticated technological capabilities are finding that it is not always possible to trace a particular message to its author. Several countries have therefore passed regulations requiring real-name user registration, whether at the point of access, via a service provider, or directly with the government. In Iran, new regulations require cybercafe customers to submit personal information before using a computer. In China, major microblogging services were given a March 2012 deadline to implement real-name registration for their users. Kazakhstan, Syria, and Saudi Arabia also passed regulations enhancing restrictions on user anonymity.

A large number of middle-performing countries—some of them democracies—are also expanding their surveillance abilities. While there are fewer fears in these settings that the government will engage in pervasive, politically motivated monitoring, rights safeguards and oversight procedures are lagging far behind the authorities' technical capacities and legal powers. For example, in a number of democratic or semidemocratic states—such as Thailand, Indonesia, Malaysia, India, and Mexico—regulations passed over the last year and a half have expanded the authority of security and intelligence services to intercept communications, sometimes without requiring a court order. Even when a judge's permission is required by law, approval is sometimes granted almost automatically due to inadequate judicial independence. In a classic example of the legal ambiguities surrounding surveillance in some countries, Indonesia has nine different laws authorizing surveillance, the most recent of which was passed in October 2011. Each law sets different standards of accountability, with only some requiring judicial approval.

The proliferation of surveillance without appropriate safeguards almost inevitably leads to abuse or inadvertent violations of user privacy. A range of countries have experienced scandals in recent years involving individual politicians or law enforcement agents who misused their powers to spy on opponents or engage in extortion. In 2011, India's federal authorities had to rein in the availability of certain interception equipment acquired after the 2008 terrorist attacks in Mumbai, as it had been improperly employed by state governments. In April 2012, Mexico's new Geolocation Law came into effect, allowing law enforcement agencies, including certain low-level public servants, to gain access to the location data of mobile phone users, without a warrant and in real time. Although such tools are intended to facilitate the apprehension of drug traffickers and violent criminals, there are credible fears that user data will fall into the wrong hands, as organized crime groups have infiltrated Mexico's law enforcement agencies. Indeed, previously collected data on mobile phone purchasers were found to have already been posted for sale online.

Even in more developed democracies, where surveillance generally requires judicial approval and oversight mechanisms are fairly robust, concerns have increased that the government is becoming too intrusive. In 2012, the British government announced a proposal to expand the existing surveillance measures and require ISPs to keep certain details of their customers' social networking activity, e-mail, internet calls, and gaming for a period of 12 months. In the United States, controversial provisions of the PATRIOT Act were renewed in May 2011, and legal ambiguities regarding data stored in the "cloud" have prompted concerns among experts. Pending legislation in Australia and South Africa has come under criticism for broadening service providers' surveillance obligations and legalizing the mass monitoring of transnational communications, respectively.

COUNTRIES AT RISK

After reviewing the findings for the 47 countries covered in this edition of *Freedom on the Net*, Freedom House has identified seven that are at particular risk of suffering setbacks related to internet freedom in late 2012 and in 2013. A number of other countries showed deterioration over the past two years and may continue to decline, but the internet controls in those states—which include Bahrain, China, Iran, Syria, and Ethiopia—are already well developed. By contrast, in most of the countries listed below, the internet remains a relatively unconstrained space for free expression, even if there has been some obstruction of internet freedom to date. These countries also typically feature a repressive environment for traditional media and have recently considered or introduced legislation that would negatively affect internet freedom.

Malaysia

Although the Malaysian government places significant restrictions on traditional media, it has actively encouraged internet and mobile phone access, resulting in an internet penetration rate of over 60 percent and a vibrant blogosphere. No politically sensitive websites are blocked, and a

notorious security law was repealed in early 2012, but other infringements on internet freedom have emerged in the last year. Prominent online news outlets and opposition-related websites have suffered cyberattacks at politically critical moments. Bloggers have faced arrest or disproportionate defamation suits for criticizing government officials or royalty. And legal amendments rendering intermediaries liable for seditious comments were passed in April 2012, as were changes to the penal code that criminalized "any activity detrimental to parliamentary democracy." In the watershed general elections of March 2008, the ruling coalition lost its two-thirds parliamentary majority for the first time since 1969, and the use of the internet for political mobilization was widely perceived as contributing to the opposition's electoral gains. As Malaysia prepares for another set of highly contentious elections scheduled to take place by April 2013, greater efforts by the government and ruling party to increase their influence over the internet are anticipated.

Russia

Given the elimination of independent television channels and the tightening of press restrictions since 2000, the internet has become Russia's last relatively uncensored platform for public debate and the expression of political opinions. However, even as access conditions have improved, internet freedom has eroded. Since January 2011, the obstacles to freedom of expression online have evolved, with massive distributed denial-of-service (DDoS) attacks, smear campaigns to discredit online activists, and extralegal intimidation of average users intensifying. Nevertheless, online tools—such as social-media networks and video-sharing platforms—played a critical role in galvanizing massive public protests that began in December 2011. The government, under the renewed leadership of President Vladimir Putin, subsequently signaled its intention to tighten control over internet communications. Since May 2012, the parliament has passed legislation that recriminalized defamation and expanded the blacklisting of websites, while prominent bloggers face detention and questionable criminal prosecutions. As the Kremlin's contentious relationship with civil society and internet activists worsens and the country prepares for regional elections in October, such controls appear likely to increase.

Sri Lanka

Although internet penetration remains at around 15 percent of the population, since 2007 there has been an incremental growth in the influence and use of online news sites and social-media tools for civic and political mobilization. The government has responded with arbitrary blocks on news websites and occasional attacks against their staff, a dynamic that has intensified since January 2011. In November, the government suddenly announced a policy requiring websites that carry "any content related to Sri Lanka" to register with the authorities, and a prominent online journalist and cartoonist remains "disappeared," apparently in police custody. The country's judicial system has proven a poor safeguard against these infringements, with the Supreme Court recently refusing to even open proceedings on a petition that challenged the arbitrary blocking of five prominent websites focused on human rights and governance. In June 2012, police raided two news websites'

offices, and in July the government announced new registration fees for such sites, illustrating the potential for further assaults on internet freedom in the coming year.

Libya

The political unrest and armed conflict in Libya, which in 2011 led to a dramatic regime change, was also reflected in the country's internet freedom landscape. The online environment was notably more open after the rebel victory in October 2011 than during the Qadhafi era or the period of civil conflict, when the internet was shut off in large areas of the country. A frenzy of self-expression has since erupted online, as Libyans seek to make up for lost time. Nevertheless, periodic electricity outages, residual self-censorship, and weak legal protections pose ongoing challenges to internet freedom. Meanwhile, the passage and subsequent overturning in mid-2012 of restrictive legislation under the guise of preventing the glorification of the Qadhafi regime highlighted the ongoing threats to online expression as different actors seek to assert their authority. Such dynamics, alongside factional fighting and recent violence in response to a YouTube video that insulted Islam, illustrate the potential pitfalls for internet freedom in Libya as the country embarks on a transition to democracy under the leadership of a new legislative body elected in July.

Azerbaijan

As the host of two high-profile international events in 2012—the Eurovision Song Contest in May and the Internet Governance Forum (IGF) in November—the government of Azerbaijan has been eager to promote itself as a leader of ICT innovation in the region. Indeed, with few websites blocked, the internet remains much less restricted than print and broadcast media, the main sources of information for most citizens. Nevertheless, as internet usage has increased dramatically over the past two years, online tools have begun to be used for political mobilization, including a series of Arab Spring–inspired prodemocracy protests in early 2011. The authorities have responded with increased efforts to clamp down on internet activities and stifle opposition viewpoints. Rather than significantly censoring online content, the government has employed tactics such as raiding cybercafes to gather information on user identities, arresting politically active netizens on trumped-up charges, and harassing activists and their family members. In a worrisome development, the authorities ramped up their surveillance capabilities in early 2012, installing "black boxes" on a mobile phone network that reportedly enable security agencies to monitor all communications in real time. While international attention on Azerbaijan's human rights record has led to some positive developments, including the recent release of imprisoned bloggers and website editors, there is concern that after the global spotlight fades, a crackdown will ensue. Furthermore, with a presidential election expected in 2013—and online tools potentially serving as an avenue for exposing electoral fraud—the risk of additional restrictions being imposed on internet freedom in Azerbaijan over the coming year remain high.

Pakistan

Mobile phones and other ICTs have proliferated in Pakistan in recent years, spurring dynamic growth in citizen journalism and activism. The government, and particularly the Pakistan Telecommunications Authority (PTA), has responded with increasingly aggressive efforts to control the new technologies. These efforts were especially pronounced between January 2011 and mid-2012, resulting in an alarming deterioration in internet freedom from the previous year. Disconcerting developments included a ban on encryption and virtual private networks (VPNs), a death sentence imposed for transmitting allegedly blasphemous content via text message, and a one-day block on all mobile phone networks in Balochistan Province in March 2012. Several other initiatives to increase censorship—including a plan to extensively filter text messages by keyword and a proposal to develop a nationwide internet firewall—were shelved after facing resistance in the form of civil society advocacy campaigns. Despite these victories, additional restrictions on internet freedom have emerged since May 2012: a brief block on Twitter, a second freeze on mobile phone networks in Balochistan, and a new PTA directive to block 15 websites featuring content about "influential persons." Evidence has also surfaced that the government is in the process of installing sophisticated internet surveillance technologies. Together, these developments signal the government's continued commitment to controlling the internet and new media. As access expands and general elections approach in April 2013, such efforts are likely to increase.

Rwanda

The government of Rwanda under President Paul Kagame has been applauded for its commitment to economic development and reconstruction since the country's devastating genocide in 1994. Investment in ICTs over the past two decades has led to the expansion of internet and mobile phone usage. Nevertheless, internet penetration remains low at only 7 percent, and widespread poverty continues to impede access to ICTs. Moreover, alongside its generally strict control over civic and political life, the government has begun exerting greater control over digital media. In the lead-up to the presidential election in 2010, the authorities blocked the online version of an independent newspaper for six months. Other online outlets have reported government requests to delete content related to political affairs or ethnic relations. Furthermore, violence against online journalists, though sporadic, appears to be on the rise, and one editor living in exile was sentenced in absentia to two and a half years in prison in June 2011. These worrying incidents have fueled concerns that the government's firm restrictions on print and broadcast media—particularly regarding content on the ruling party or the 1994 genocide—are crossing over into the internet sphere. In one ominous sign, in August 2012 the government approved legislation that, if passed by the Senate, would enable security and intelligence services to conduct widespread surveillance of e-mail and telephone communications.