DESPITE PUSHBACK, INTERNET FREEDOM DETERIORATES

By Sanja Kelly

In June 2013, revelations made by former contractor Edward Snowden about the U.S. government's secret surveillance activities took center stage in the American and international media. As part of its antiterrorism effort, the U.S. National Security Agency (NSA) has been collecting communications data on Americans and foreigners on a much greater scale than previously thought. However, while the world's attention is focused on Snowden and U.S. surveillance—prompting important discussions about the legitimacy and legality of such measures—disconcerting efforts to both monitor and censor internet activity have been taking place in other parts of the world with increased frequency and sophistication. In fact, global internet freedom has been in decline for the three consecutive years tracked by this project, and the threats are becoming more widespread.

Global internet freedom has been in decline for the three consecutive years tracked by this project.

Of particular concern are the proliferation of laws, regulations, and directives to restrict online speech; a dramatic increase in arrests of individuals for something they posted online; legal cases and intimidation against social-media users; and a rise in surveillance. In authoritarian states, these tools are often used to censor and punish users who engage in online speech that is deemed critical of the government, royalty, or the dominant religion. In some countries, even blogging about environmental pollution, posting a video of a cynical rap song, or tweeting about the town mayor's poor parking could draw the police to a user's door. Although democratic states generally do not target political speech, several have sought to implement disproportionate restrictions on content they perceive as harmful or illegal, such as pornography, hate speech, and pirated media.

In some countries, even posting a video of a cynical rap song could draw the police to a user's door.

Nonetheless, in a number of places around the world, growing efforts by civic activists, technology companies, and everyday internet users have been able to stall, at least in part, newly proposed restrictions, forcing governments to either shelve their plans or modify some of the more problematic aspects of draft legislation. In a handful of countries, governments have been increasingly open to engagement with civil society, resulting in the passage of laws perceived to protect internet freedom. While such

Sanja Kelly directs the *Freedom on the Net* project at Freedom House.

positive initiatives are significantly less common than government attempts to control the online sphere, the expansion of this movement to protect internet freedom is one of the most important developments of the past year.

To illuminate the nature of evolving threats in the rapidly changing global environment, and to identify areas of opportunity for positive change, Freedom House has conducted a comprehensive study of internet freedom in 60 countries around the world. This report is the fourth in its series and focuses on developments that occurred between May 2012 and April 2013. The previous edition, covering 47 countries, was published in September 2012. *Freedom on the Net 2013* assesses a greater variety of political systems than its predecessors, while tracing improvements and declines in the countries examined in the 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 60 countries assessed, 34 have experienced a negative trajectory since May 2012.

Of the 60 countries assessed, 34 have experienced a negative trajectory since May 2012. Further policy deterioration was seen in authoritarian states such as Vietnam and Ethiopia, where the downgrades reflected new government measures to restrict free speech, new arrests, and harsh prison sentences imposed on bloggers for posting articles that were critical of the authorities. Pakistan's downgrade reflected the blocking of thousands of websites and pronounced violence against users of information and communication technologies (ICTs). In Venezuela, the decline was caused by a substantial increase in censorship surrounding politically sensitive events: the death of President Hugo Chávez and the presidential elections that preceded and followed it.

Deterioration was also observed in a number of democracies, often as a result of struggles to balance freedom of expression with security. The most significant year-on-year decline was seen in India, which suffered from deliberate interruptions of mobile and internet service to limit unrest, excessive blocks on content during rioting in northeastern states, and an uptick in the filing of criminal charges against ordinary users for posts on social-media sites. The United States experienced a significant decline as well, in large part due to reports of extensive surveillance tied to intelligence gathering and counterterrorism. And in Brazil, declines resulted from increasing limitations on online content, particularly in the context of the country's stringent electoral laws; cases of intermediary liability; and increasing violence against online journalists.

Deterioration was also observed in a number of democracies, often as a result of struggles to balance freedom of expression with security.

At the same time, 16 countries registered a positive trajectory over the past year. In Morocco, which was analyzed for the first time in this edition of the report, the government has unblocked previously censored websites as part of its post–Arab Spring reform effort, although it still frequently punishes those who post controversial information. Burma's continued improvement included significant steps toward the lifting of internet censorship, which may allow the country to

shed its history of repression and underdevelopment and create a more progressive media environment. Tunisia's gains are the result of the government's sustained efforts to open up the online sphere following years of repression under former president Zine el-Abidine Ben Ali, and institute protections for journalists and bloggers, although there is still much to be done. And in several countries like Georgia and Rwanda, improvements stemmed from a decline in the number of negative incidents from the previous coverage period.

Despite the noted improvements, restrictions on internet freedom continue to expand across a wide range of countries. Over the past year, the global number of censored websites has increased, while internet users in various countries have been arrested, tortured, and killed over the information they posted online. Iran, Cuba, and China remain among the most restrictive countries in the world when it comes to internet freedom. In Iran, the government utilized more advanced methods for blocking text messages, filtering content, and preventing the use of circumvention tools in advance of the June 2013 election, while one blogger was found dead in police custody after being arrested for criticizing the government online. In Cuba, the authorities continued to require a special permit for anyone wishing to access the global internet; the permits are generally granted to trusted party officials and those working in specific professions. And as in previous years, China led the way in expanding and adapting an elaborate technological apparatus for systemic internet censorship, while further increasing offline coercion and arrests to deter free expression online.

Over the past year, the global number of censored websites has increased, while internet users in various countries have been arrested, tortured, and killed over the information they posted online.

Based on a close evaluation of each country, this study identifies the 10 most commonly used types of internet control, most of which appear to have become more widespread over the past year:

Blocking and filtering:

Governments around the world are increasingly establishing mechanisms to block what they deem to be undesirable information. In many cases, the censorship targets content involving child pornography, illegal gambling, copyright infringement, or the incitement of violence. However, a growing number of governments are also engaging in deliberate efforts to block access to information related to politics, social issues, and human rights. Of the 60 countries evaluated this year, 29 have used blocking to suppress certain types of political and social content. China, Iran, and Saudi Arabia possess some of the most comprehensive blocking and filtering capabilities, effectively disabling access to thousands of websites, but even some democratic countries like South Korea and India have at times blocked websites of a political nature. Jordan and Russia, which previously blocked websites only sporadically, are among the countries that have intensified their efforts over the past year.

Cyberattacks against regime critics:

Some governments and their sympathizers are increasingly using technical attacks to disrupt activists' online networks, eavesdrop on their communications, and cripple their websites. Over the past year, such attacks were reported in at least 31 of the countries covered in this study. In Venezuela, for example, during the 2012 and 2013 presidential campaigns, the websites of popular independent media—Noticiero Digital, Globovisión, and La Patilla—were repeatedly subject to distributed denial-of-service (DDoS) attacks, which increased on election days and during the vote count. In countries ranging from Belarus to Vietnam to Bahrain, opposition figures and activists are routinely targeted with malicious software that is masked as important information about political developments or planned protests. When downloaded, the malware can enable attackers to monitor the victims' keystrokes and eavesdrop on their personal communications. Although activists are increasingly aware of this practice and have been taking steps to protect themselves, the attacks are becoming more sophisticated and harder to detect.

New laws and arrests for political, religious, or social speech online:

Instead of merely blocking and filtering information that is deemed undesirable, an increasing number of countries are passing new laws that criminalize certain types of political, religious, or social speech, either explicitly or through vague wording that can be interpreted in such a way. Consequently, more users are being arrested, tried, or imprisoned for their posts on social networks, blogs, and websites. In fact, some governments may prefer to institute strict punishments for people who post offending content rather than actually blocking it, as this allows officials to maintain the appearance of a free and open internet while imposing a strong incentive for users to practice self-censorship. Even countries willing to invest in systematic filtering often find that criminal penalties remain an important deterrent. Turkey, Bangladesh, and Azerbaijan are among the countries that have, over the past year, significantly stepped up arrests of users for their online activism and posts.

More users are being arrested, prosecuted, or imprisoned for their posts on social networks, blogs, and websites.

Paid progovernment commentators manipulate online discussions:

Already evident in a number of countries assessed in the previous edition of *Freedom of the Net*, the phenomenon of paid progovernment commentators has spread in the past two years, appearing in 22 of the 60 countries examined in this study. The purpose of these commentators—covertly hired by government officials, often by using public funds—is to manipulate online discussions by trying to smear the reputation of government opponents, spread propaganda, and defend government policies when the discourse becomes critical. China, Bahrain, and Russia have been at the forefront of this practice for several years, but countries like Malaysia, Belarus, and Ecuador are increasingly using the same tactics, particularly surrounding politically sensitive events such as elections or major street protests.

Physical attacks and murder:

Governments and powerful nonstate actors are increasingly resorting to physical violence to punish those who disseminate critical content, with sometimes fatal consequences. In 26 of the 60 countries assessed, at least one blogger or internet user was attacked, beaten, or tortured for something posted online. In 5 of those countries, at least one activist or citizen journalist was killed in retribution for information posted online, in most cases information that exposed human rights abuses. Syria was the most dangerous place for online reporters, with approximately 20 killed over the past year. In Mexico, several online journalists were murdered after refusing to stop writing exposés about drug trafficking and organized crime. In Egypt, several Facebook group administrators were abducted and beaten, while citizen journalists were allegedly targeted by the security forces during protests.

In 5 countries, at least one activist or citizen journalist was killed in retribution for information posted online.

Surveillance:

Many governments are seeking less visible means to infringe on internet freedom, often by increasing their technical capacity or administrative authority to monitor individuals' online behavior or communications. Governments across the spectrum of democratic performance have enhanced their surveillance capabilities in recent years or have announced their intention to do so. Although some interception of communications may be necessary for fighting crime or preventing terrorist attacks, surveillance powers are increasingly abused for political ends. Governments in nearly two-thirds of the countries examined upgraded their technical or legal surveillance powers over the past year (see surveillance section in "Major Trends" below). It is important to note that increased surveillance, particularly in authoritarian countries where the rule of law is weak, often leads to increased self-censorship, as users become hesitant to risk repercussions by criticizing the authorities online.

Governments across the spectrum of democratic performance have enhanced their surveillance capabilities in recent years.

Takedown requests and forced deletion of content:

Instead of blocking objectionable websites, many governments opt to contact the content hosts or social-media sites and request that the content be "taken down." While takedown notices can be a legitimate means of dealing with illegal content when the right safeguards are in place, many governments and private actors are abusing the practice by threatening legal action and forcing the removal of material without a proper court order. A more nefarious activity, which is particularly common in authoritarian countries, involves government officials informally contacting a content producer or host and requesting that particular information be deleted. In some cases, individual bloggers or webmasters are threatened with various reprisals should they refuse. In Russia and Azerbaijan, for example, bloggers have reported deleting comments from their websites after being told that they would be fired from their jobs, barred from universities, or detained if they did not comply.

Blanket blocking of social media and other ICT platforms:

Given the increasing role that social media have played in political and social activism, particularly after the events of the Arab Spring, some governments have been specifically targeting sites like YouTube, Twitter, and Facebook in their censorship campaigns. In 19 of the 60 countries examined, the authorities instituted a blanket ban on at least one blogging, microblogging, video-sharing, social-networking, or live-streaming platform. However, as their knowledge and sophistication grows, some governments are beginning to move toward blocking access to individual pages or profiles on such services or requesting from the companies to disable access to the offending content. These dynamics were particularly evident surrounding protests that erupted after the anti-Islam video *Innocence of Muslims* appeared on YouTube. Voice over Internet Protocol (VoIP) and free messaging services such as Skype, Viber, and WhatsApp are also frequently targeted—in some countries due to difficulties the authorities face in intercepting such communication tools, and in others because the telecommunications industry perceives them as a threat to their own revenue. Lebanon, Ethiopia, and Burma are among several countries where the use of VoIP services remained prohibited as of May 2013.

Holding intermediaries liable:

An increasing number of countries are introducing directives, passing laws, or interpreting current legislation so as to make internet intermediaries—whether internet service providers (ISPs), site hosting services, webmasters, or forum moderators—legally liable for the content posted by others through their services and websites. As a consequence, intermediaries in some countries are voluntarily taking down or deleting potentially objectionable websites or comments 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 social-media sites, search engines, and online forums, deleting tens of millions of messages a year based on administrators' interpretation of both long-standing taboos and daily directives from the ruling Communist Party. In 22 of the 60 countries examined, intermediaries were held to a disproportionate level of liability, either by laws that clearly stipulate such rules or by court decisions with similar effects. In one recent example, Brazilian authorities issued arrest warrants for two senior Google Brazil executives on the grounds that the company failed to remove content that was prohibited under strict laws governing electoral campaigns.

Intermediaries in some countries are voluntarily taking down or deleting potentially objectionable websites or comments to avoid legal liability.

Throttling or shutting down internet and mobile service:

During particularly contentious events, a few governments have used their control over the telecommunications infrastructure to cut off access to the internet or mobile phone service in a town, a region, or the entire country. Egypt became the best-known case study in

January 2011, when the authorities shut off the internet for five days as protesters pushed for the ouster of longtime president Hosni Mubarak. However, a number of other countries have also cut off access to the internet or mobile phone networks. In Syria, several such shutdowns occurred over the past year. In Venezuela, the dominant ISP temporarily shut off access during the presidential election in 2012, allegedly due to cyberattacks. India and China disabled text messaging on mobile phones in particular regions during protests and rioting. In addition to outright shutdowns, some countries have used throttling, the deliberate slowing of connection speeds, to prevent users from uploading videos or viewing particular websites without difficulty. Over the past year, however, there were fewer instances of internet shutdowns and throttling than in the previous year, most likely because countries affected by the Arab Spring in 2011 had moved past the point where such tactics would be useful to the authorities.

MAJOR TRENDS

Although many different types of internet control have been institutionalized in recent years, three particular trends have been at the forefront of increased censorship efforts: increased surveillance, new laws that restrict online speech, and arrests of users. Despite these threats, civic activism has also been on the rise, providing grounds for hope that the future may bring more positive developments.

Surveillance grows considerably as countries upgrade their monitoring technologies

Starting in June 2013, a series of leaks by former U.S. contractor Edward Snowden revealed that the NSA was storing the personal communications metadata of Americans—such as the e-mail addresses or phone numbers on each end, and the date and time of the communication—and mining them for leads in antiterrorism investigations. Also exposed were details of the PRISM program, through which, among other things, the NSA monitored communications of non-Americans via products and services offered by U.S. technology companies. It then came to light that several other democratic governments had their own surveillance programs aimed at tracking national security threats and cooperating with the NSA. While there is no evidence that the NSA surveillance programs were abused to suppress political speech, they have drawn strong condemnations at home and abroad for their wide-reaching infringements on privacy. Since many large technology companies—with millions of users around the world—are based in the United States, the NSA was able to collect information on foreigners without having to go through the legal channels of the countries in which the targeted users were located.

Although the U.S. surveillance activities have taken the spotlight in recent months, this study reveals that most countries around the world have enhanced their surveillance powers over the past year. In 35 of the 60 countries examined in *Freedom on the Net 2013*, the government has either obtained more sophisticated technology to conduct surveillance, increased the scope and number of people monitored, or passed a new law giving it greater monitoring authority. There is a strong suspicion that many of the remaining 25 countries' governments have also stepped up their surveillance activities, though some may be better than others at covering their tracks.

In 35 of the 60 countries examined, the government has obtained more sophisticated surveillance technology, increased the scope of people monitored, or passed a new law giving it greater monitoring authority. Growing surveillance is also suspected in many of the remaining 25 countries, but they may be better at covering their tracks.

While democratic countries have often engaged in legally dubious surveillance methods to combat and uncover terrorism threats, officials in many authoritarian countries also monitor the personal communications of their citizens for political reasons, with the goal of 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 Bahrain, Ethiopia, Azerbaijan, and elsewhere, activists reported that their e-mail, text messages, or other communications were presented to them during interrogations or used as evidence in politicized trials. In many of these countries, the state owns the main telecommunications firms and ISPs, and it does not have to produce a warrant from an impartial court to initiate surveillance against dissidents.

Russia has emerged as an important incubator of surveillance technologies and legal practices that are emulated by other former Soviet republics. Russia itself has dramatically expanded its surveillance apparatus in recent years, particularly following the events of the Arab Spring. Moreover, in December 2012, the Russian Supreme Court upheld the legality of the government's hacking into the phone of an opposition activist. The court grounded its decision on the fact that the activist had participated in antigovernment rallies, prompting fears that the case would be used as a legal basis for even more extensive surveillance against opposition figures in the future. Belarus, Uzbekistan, Kyrgyzstan, Kazakhstan, and Ukraine are among the countries that have implemented the ICT monitoring system used by the Russians authorities (known by the acronym SORM) and have either passed or considered legislation that would further expand their surveillance powers, in some cases mimicking the current legislation in Russia.

All 10 of the African countries examined in this report have stepped up their online monitoring efforts in the past year.

Until recently, only a handful of African countries had the means to conduct widespread surveillance. However, this seems to be changing rapidly as internet penetration increases and surveillance technologies become more readily available. All 10 of the African countries examined in this report have stepped up their online monitoring efforts in the past year, either by obtaining new technical capabilities or by expanding the government's legal authority. In Sudan, the government's ICT surveillance was particularly pronounced in 2012

during a series of street protests, and it became dangerous for activists to use their mobile phones. One activist switched off his phone for a few days to avoid arrest while hiding from the authorities. When he turned it back on to call his family, officials quickly determined his location and arrested him the same day.

In the Middle East and North Africa, where extralegal surveillance has long been rampant, the authorities continue to use ICT monitoring against regime opponents. In Saudi Arabia, the government has been proactively recruiting experts to work on intercepting encrypted data from mobile applications such as Twitter, Viber, Vine, and WhatsApp. In Egypt, President Mohamed Morsi's advisers reportedly met with the Iranian spy chief in December 2012 to seek assistance in building a surveillance apparatus that would be controlled by the office of the president and operated outside of traditional security structures. Even in postrevolutionary Libya, reports surfaced in mid-2012 that surveillance tools left over from the Qadhafi era had been restored, apparently for use against suspected loyalists of the old regime.

Perhaps most worrisome is the fact that an increasing number of countries are using malware to conduct surveillance when traditional methods are less effective. Opposition activists in the United Arab Emirates, Bahrain, Malaysia, and more than a dozen other countries were targeted with malware attacks over the past year, giving the attackers remote access to victims' e-mail, keystrokes, and voice communications. While it is difficult to know with a high degree of certainty, there are strong suspicions that these activists' respective governments were behind the attacks. Some democratic governments—including in the United States and Germany—have used malware to conduct surveillance in criminal investigations, but any such use typically must be approved by a court order and narrowly confined to the scope of the investigation.

Censorship intensifies as countries pass new laws and directives to restrict online speech

Until several years ago, very few countries had laws that specifically dealt with ICTs. As more people started to communicate online—particularly via social media, which allow ordinary users to share information on a large scale—an increasing number of governments have introduced new laws or amended existing statutes to regulate speech and behavior in cyberspace. Since launching *Freedom on the Net* in 2009, Freedom House has observed a proliferation of such legislative activity. This trend accelerated over the past year, and since May 2012 alone, 24 countries have passed new laws or implemented new regulations that could restrict free speech online, violate users' privacy, or punish individuals who post certain types of content.

24 countries have passed new laws or implemented new regulations that could restrict free speech online, violate users' privacy, or punish individuals who post certain types of content.

Many authoritarian countries have used legitimate concerns about cybercrime and online identity theft to introduce new legal measures that criminalize critical political speech. In November 2012, the government of the United Arab Emirates issued a new cybercrime law that provides a sounder legal basis for combatting

online fraud, money laundering, hacking, and other serious abuses. However, the law also contains punishments for offending the state, its rulers, and its symbols, and for insulting Islam and other religions. Those found guilty of calling for a change to the ruling system can face a sentence of life in prison. In September 2012, Ethiopia's government passed the Telecom Fraud Offenses law, which is supposed to combat cybercrime but also includes provisions that toughen the ban on VoIP, require users to register all ICT equipment (including smartphones) and carry registration permits with them, and apply penalties under an antiterrorism law to certain types of electronic communications. Considering that free speech activists have already been tried under the antiterrorism laws for criticism of the regime, the new legislation was met with significant concern.

Several countries have also passed new laws intended to block information that is perceived as "extremist" or harmful to children. While such concerns have led to legitimate policy discussions in a wide range of countries, some of the recent legislation is so broadly worded that it can easily be misused or turned on political dissidents. For example, the Russian parliament in July 2012 passed what is commonly known as the "internet blacklist law," which allows blocking of any website with content that is considered harmful to minors, such as child pornography and information related to suicide techniques and illegal drug use. However, the law has also been used occasionally to block other websites, such as a blog by an opposition figure (no official reason for blocking was provided) or another blog that featured a photo-report on the self-immolation of a Tibetan independence activist protesting the visit of the Chinese president (the official reason for blocking was that the post promoted suicide). In Kyrgyzstan, a new law allows the government to order web hosting services to shut down websites hosted in Kyrgyzstan, or the blocking of any sites hosted outside the country, if officials recognize the content as "extremist," which is very broadly defined.

In some countries, the authorities have decided to institute stricter regulations specifically aimed at online news media. The traditional media in authoritarian states are typically controlled by the government, and users often turn to online news outlets for independent information. The tighter controls are designed to help rein in this alternative news source. A new law in Jordan requires any electronic outlet that publishes domestic or international news, press releases, or comments to register with the government; it places conditions on who can be the editor in chief of such outlets; and it prohibits foreign investment in news media. The penalties for violations include fines and blocking, and in May 2013 the government proceeded to block over 200 websites that failed to comply with the new rules. Similarly, in Sri Lanka, online news outlets are now required to obtain a license, which can be denied or withdrawn at any time.

More users are arrested, and face harsher penalties, for posts on social media

Laws that restrict free speech are increasingly forcing internet users into courts or behind bars. Over the past year alone, in 28 of the 60 countries examined, at least one user was arrested or imprisoned for posting certain types of political, social, or religious content online. In fact, a growing number of governments seem to exert control over the internet not through blocking and filtering, but by arresting people after the posts are published online. In addition, courts in some

In 28 of the 60 countries examined, at least one user was arrested or imprisoned for posting political, social, or religious content online.

countries have allowed higher penalties for online speech than for equivalent speech offline, arguably because of the internet's wider reach.

As more people around the world utilize social media to express their opinions and communicate with others, there has been a dramatic increase in arrests for posts on sites such as Twitter, Facebook, and YouTube. In at least 26 of the examined countries, users were arrested for politically or socially relevant statements on social-media sites. Although political activists are targeted most frequently, more and more ordinary, apolitical users have found themselves in legal trouble after casually posting their opinions and jokes. Unlike large media companies and professional journalists with an understanding of the legal environment, many users of this kind may be unaware that their writings could land them in jail.

Last year in India, for example, at least eleven users were charged under the so-called IT Act for posting or "liking" posts on Facebook. In one of the best-known cases, police arrested a woman for complaining on Facebook about widespread traffic and service disruptions in her town to mark the death of the leader of a right-wing Hindu nationalist party. The woman's friend, who "liked" the comment, was also arrested. The detentions were widely criticized, both on social media and by public figures, and the charges were later dropped. In Ethiopia, a student was arrested and charged with criminal defamation after he posted a comment on his Facebook page that criticized the "rampant corruption" at another local university.

A woman in India was arrested for "liking" a friend's status on Facebook.

Users are most often detained and tried for simply criticizing or mocking the authorities. At least 10 users were arrested in Bahrain over the past year and charged with "insulting the king on Twitter," and several ultimately received prison sentences ranging from one to four months. In Morocco, an 18-year-old student was sentenced to 18 months in prison for "attacking the nation's sacred values" after he allegedly ridiculed the king in a Facebook post, and a 25-year-old activist received an even harsher sentence for criticizing the king in a YouTube video. In Vietnam, several bloggers were sentenced to between 8 and 13 years in prison on charges that included "defaming state institutions" and "misuse of democratic freedoms to attack state interests."

In addition to criticism of political leaders, speech that might offend religious sensitivities is landing a growing number of users in jail. This is most prevalent in the Middle East, but it has occurred elsewhere in the world. In Saudi Arabia, any discussion that questions the official interpretation of Islam commonly leads to arrest. Prominent writer Turki al-Hamad was arrested in December 2012 after tweeting that "we need someone to rectify the doctrine of [the prophet] Muhammad;" he was held in detention for five months. In April 2013, a Tunisian court upheld a prison sentence of seven and a half years for a man who published cartoons depicting the prophet Muhammad on his Facebook page. And earlier this year in Bangladesh, several bloggers were charged with "harming religious sentiments" under the country's ICT Act for openly atheist posts that criticized Islam. The

charges carried a prison sentence of up to 10 years, though in August 2013 the law was amended to increase the maximum penalty to 14 years.

Some regimes have also shown very little tolerance for humor that may cast them or the country's religious authorities in a negative light, leading to more arrests and prosecutions. For instance, in June 2012, a popular Turkish composer and pianist was charged with offending Muslims with his posts on Twitter, including one in which he joked about a call to prayer that lasted only 22 seconds, suggesting that the religious authorities had been in a hurry to get back to their drinking and mistresses. He was charged with inciting hatred and insulting "religious values," and received a suspended sentence of 10 months in prison. In another example, in India, a 25-year-old cartoonist was arrested on a charge of sedition—which carries a life sentence—and for violating laws against insulting national honor through his online anticorruption cartoons, one of which depicted the national parliament as a toilet. He was released on bail after the sedition charge was dropped.

Growing activism stalls negative proposals and promotes positive change

Although threats to internet freedom have continued to grow, the study's findings also reveal a significant uptick in citizen activism online. While it has not always produced legislative changes—in fact, negative developments in the past year vastly outnumber positive developments—there is a rising public consciousness about internet freedom and freedom of expression issues. Citizens' groups are able to more rapidly disseminate information about negative proposals and put pressure on the authorities. In addition, ICTs have started to play an important role in advocacy for positive change on other policy topics, from corruption to women's rights, enabling activists and citizens to more effectively organize, lobby, and hold their governments accountable.

This emergent online activism has taken several forms. In 11 countries, negative laws were deterred as a result of civic mobilization and pressure by activists, lawyers, the business sector, reform-minded politicians, and the international community. In the Philippines, after the passage of the restrictive Cybercrime Prevention Act, online protests and campaigns ran for several months. Individuals blacked out their profile pictures on social networks, and 15 petitions were filed with the Supreme Court, which eventually put a restraining order on the law, deeming it inapplicable in practice. In Kyrgyzstan, the government proposed a law on protection of children—modeled on the similar law in Russia—that activists feared would be used as a tool for internet censorship, as it allowed the government to close sites without a court decision. The proposal sparked public outrage, spurring local advocacy efforts that eventually compelled parliament to postpone the bill until it could be amended.

In 11 countries, negative laws were deterred as a result of civic mobilization and pressure by activists, lawyers, the business sector, reform-minded politicians, and the international community.

In a select few countries, civic activists were able to form coalitions and proactively lobby governments to pass laws that protect internet freedom or amend previously restrictive legislation.

In Mexico, for example, following a public campaign by 17 civil society organizations that joined forces in early 2013, freedom of access to the internet in now guaranteed in Article 6 of the constitution. Although the Mexican government has not introduced any secondary legislation that would specify how the new right will be protected in practice, the constitutional amendment is seen as a significant victory. In the United Kingdom, the government passed a law to revise the Defamation Act, discouraging the practice of "libel tourism" and limiting intermediary liability for user-generated content of defamatory nature. Civil society has also been increasingly active on the global stage, lobbying for greater transparency and inclusion in advance of the World Conference on International Telecommunications (WCIT-12) in Dubai, and in some instances placing pressure on their national delegations.

ICTs have also been an important tool for mobilization on issues other than internet freedom, leading to important changes. In Morocco, online activism contributed to a national debate on Article 475 of the penal code, which allows rapists to avoid prosecution if they agree to marry their victims. Although women's rights advocates have been lobbying for years to alter this law, the necessary momentum was created only after a 16-year-old girl committed suicide, having been forced to wed her alleged rapist. Women's rights activists successfully used social media and online news platforms to counter arguments made by state-controlled radio and television outlets, rallying popular support for reforms. In January 2013, the government announced plans to revise the article in question. In other countries—including many authoritarian states like China, Saudi Arabia, and Bahrain—citizen journalists' exposés of corruption, police abuse, pollution, and land grabs forced the authorities to at least acknowledge the problem and in some cases punish the perpetrators.

In addition to activism by groups, citizens, and other stakeholders, the judiciary has played an important role as protector of internet freedom, particularly in more democratic countries where the courts operate with a greater degree of independence. Since May 2012, the courts in at least 9 countries have issued decisions that may have a positive impact on internet freedom. In South Korea, the Constitutional Court overturned a notorious law that required all users to register with their real names when commenting on large websites. In Italy, a court issued a ruling to clarify that blogs cannot be considered illegal "clandestine press" under an outdated law stipulating that anyone providing a news service must be a "chartered" journalist. In practice this rule had led some bloggers and internet users to collaborate with registered journalists when publishing online in order to protect themselves from legal action.