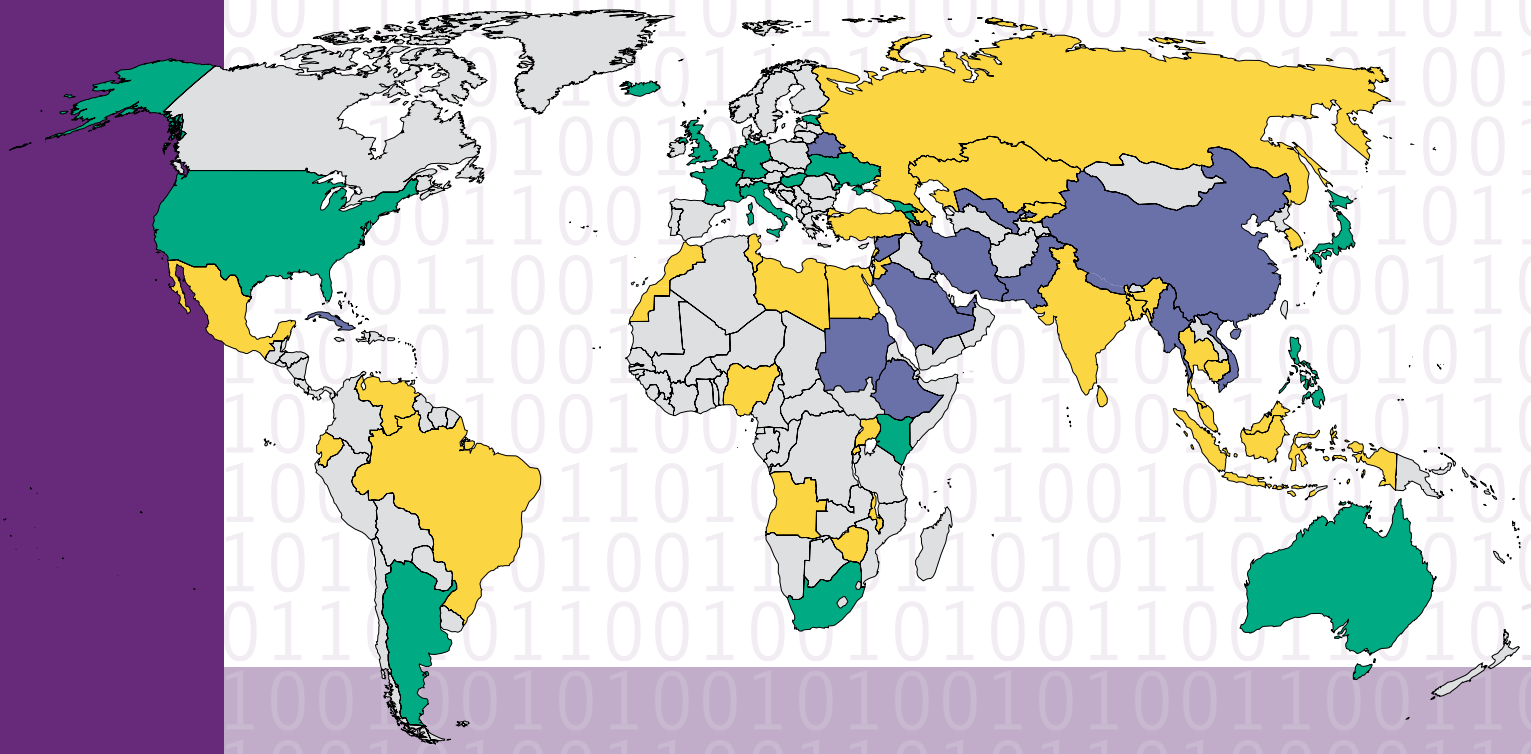
FREEDOM HOUSE

FREEDOM ON THE NET 2013

A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA



SUMMARY OF FINDINGS

www.freedomhouse.org

FREEDOM ON THE NET 2013

A Global Assessment of Internet and Digital Media

Sanja Kelly
Mai Truong
Madeline Earp
Laura Reed
Adrian Shahbaz
Ashley Greco-Stoner

EDITORS

October 3, 2013

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), and Google. 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, or Google.

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.

KEY INTERNET CONTROLS BY COUNTRY

Country (By FOTN 2013 ranking)	FOTN 2013 Status (F=Free, PF=Partly Free, NF=Not Free)	Social media and/or communication apps blocked	Political, social, and/or religious content blocked	Localized or nationwide ICT shutdown	Progovernment commentators manipulate online discussions	New law /directive increasing censorship or punishment passed	New law /directive incr. surveillance or restricting anonymity passed	Blogger/ICT user arrested for political or social writings	Blogger/ICT user physically attacked or killed (incl. in custody)	Technical attacks against government critics and human rights orgs
Iceland	F									
Estonia	F									
Germany	F						X			
USA	F									
Australia	F						X			
France	F									
Japan	F					X				
Hungary	F					X			X	
Italy	F									
UK	F									
Philippines	F					X	X			
Georgia	F									
South Africa	F						X			
Argentina	F								X	X
Kenya	F									
Ukraine	F							X	X	X
Armenia	F									X
Nigeria	PF									
Brazil	PF							X	X	
South Korea	PF		X		X					
Angola	PF								X	X
Uganda	PF									X
Kyrgyzstan	PF		X		X				X	
Ecuador	PF				X	X	X		X	X
Mexico	PF				X			X	X	X
Indonesia	PF		X							
Tunisia	PF							X		X
Malawi	PF				X			X		
Morocco	PF				X			X	X	X
Malaysia	PF		X		X			X		X

Country (By FOTN 2013 ranking)	FOTN 2013 Status (F=Free, PF=Partly Free, NF=Not Free)	Social media and/or communication apps blocked	Political, social, and/or religious content blocked	Localized or nationwide ICT shutdown	Progovernment commentators manipulate online discussions	New law /directive increasing censorship or punishment passed	New law /directive incr. surveillance or restricting anonymity passed	Blogger/ICT user arrested for political or social writings	Blogger/ICT user physically attacked or killed (incl. in custody)	Technical attacks against government critics and human rights orgs
Lebanon	PF	X						X	X	X
Libya	PF		X						X	
Jordan	PF					X				X
Cambodia	PF		X							
India	PF	X	X	X	X			X		
Rwanda	PF		X			X				
Bangladesh	PF	X	X			X		X	X	X
Turkey	PF	X	X					X		
Azerbaijan	PF	X	X				X	X		
Venezuela	PF		X	X	X			X	X	X
Russia	PF		X		X	X		X	X	X
Zimbabwe	PF							X		X
Sri Lanka	PF		X			X		X	X	X
Kazakhstan	PF	X	X		X					X
Egypt	PF				X			X	X	X
Thailand	PF		X		X		X			
Burma	NF	X								X
Sudan	NF	X	X		X			X	X	X
UAE	NF	X	X			X		X	X	X
Belarus	NF	X	X		X			X	X	X
Pakistan	NF	X	X	X			X		X	
Saudi Arabia	NF	X	X		X		X	X		X
Bahrain	NF	X	X		X			X	X	X
Vietnam	NF		X		X	X	X	X	X	X
Uzbekistan	NF	X	X		X	X				X
Ethiopia	NF	X	X		X	X		X		X
Syria	NF	X	X	X				X	X	X
China (PRC)	NF	X	X	X	X		X	X	X	X
Cuba	NF	X	X		X	X		X	X	
Iran	NF	X	X					X	X	X
TOTAL		19	29	5	22	14	11	28	26	31

X = Internet control observed during the May 2012 – April 2013 coverage period;
X = Internet control observed after May 1, 2013

KEY INTERNET CONTROLS BY COUNTRY

CHARTS AND GRAPHS OF KEY FINDINGS

Freedom on the Net measures the level of internet and digital media freedom in 60 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of **FREE (0-30 points)**, **PARTLY FREE (31-60 points)**, or **NOT FREE (61-100 points)**.

Ratings are determined through an examination of three broad categories:

A. **OBSTACLES TO ACCESS:** assesses infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; and legal, regulatory, and ownership control over internet and mobile phone access providers.
B. **LIMITS ON CONTENT:** examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
C. **VIOLATIONS OF USER RIGHTS:** measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

FREEDOM ON THE NET 2013: GLOBAL SCORES

COUNTRY	FREEDOM ON THE NET 2013 STATUS	FREEDOM ON THE NET 2013 TOTAL *0-100 Points*	A. SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B. SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C. SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
ICELAND	Free	6	1	1	4
ESTONIA	Free	9	1	3	5
GERMANY	Free	17	4	4	9
UNITED STATES	Free	17	4	1	12
AUSTRALIA	Free	18	2	5	11
FRANCE	Free	20	4	4	12
JAPAN	Free	22	4	7	11
HUNGARY	Free	23	5	8	10
ITALY	Free	23	5	6	12
UNITED KINGDOM	Free	24	2	6	16

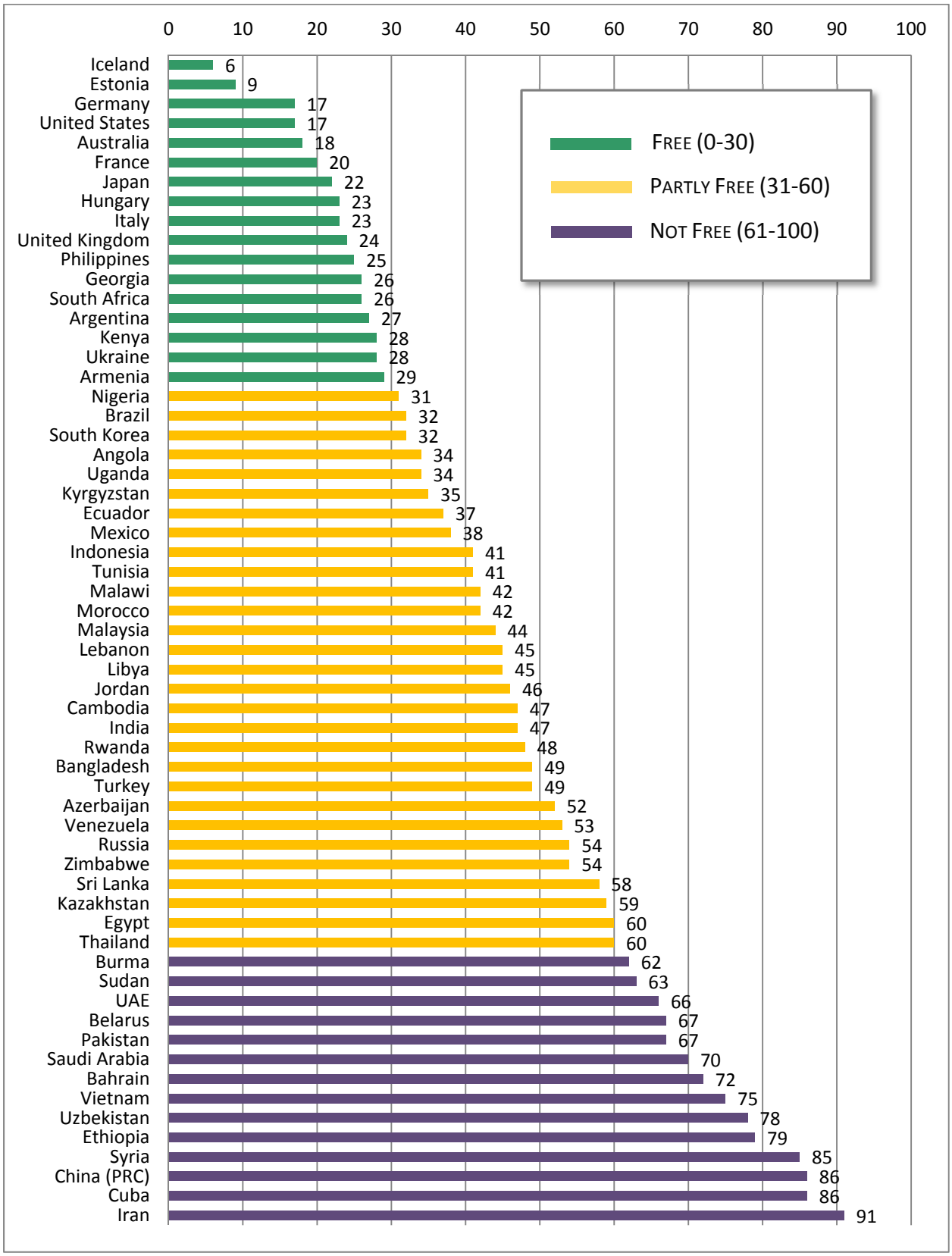
COUNTRY	FREEDOM ON THE NET 2013 STATUS	FREEDOM ON THE NET 2013 TOTAL *0-100 Points*	A. SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B. SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C. SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
PHILIPPINES	Free	25	10	5	10
GEORGIA	Free	26	8	7	11
SOUTH AFRICA	Free	26	7	8	11
ARGENTINA	Free	27	8	10	9
KENYA	Free	28	9	7	12
UKRAINE	Free	28	7	7	14
ARMENIA	Free	29	8	9	12
NIGERIA	Partly Free	31	10	8	13
BRAZIL	Partly Free	32	7	8	17
SOUTH KOREA	Partly Free	32	3	13	16
ANGOLA	Partly Free	34	15	6	13
UGANDA	Partly Free	34	11	8	15
KYRGYZSTAN	Partly Free	35	12	10	13
ECUADOR	Partly Free	37	10	11	16
MEXICO	Partly Free	38	11	10	17
INDONESIA	Partly Free	41	11	11	19
TUNISIA	Partly Free	41	12	8	21
MALAWI	Partly Free	42	16	11	15
MOROCCO	Partly Free	42	11	7	24
MALAYSIA	Partly Free	44	9	15	20
LEBANON	Partly Free	45	14	10	21
LIBYA	Partly Free	45	17	9	19
JORDAN	Partly Free	46	13	13	20
CAMBODIA	Partly Free	47	14	15	18
INDIA	Partly Free	47	15	12	20

CHARTS AND GRAPHS OF KEY FINDINGS

COUNTRY	FREEDOM ON THE NET 2013 STATUS	FREEDOM ON THE NET 2013 TOTAL *0-100 Points*	A. SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B. SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C. SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
RWANDA	Partly Free	48	12	18	18
BANGLADESH	Partly Free	49	13	12	24
TURKEY	Partly Free	49	12	18	19
AZERBAIJAN	Partly Free	52	13	17	22
VENEZUELA	Partly Free	53	16	16	21
RUSSIA	Partly Free	54	10	19	25
ZIMBABWE	Partly Free	54	16	14	24
SRI LANKA	Partly Free	58	15	20	23
KAZAKHSTAN	Partly Free	59	15	23	21
EGYPT	Partly Free	60	15	12	33
THAILAND	Partly Free	60	10	21	29
BURMA	Not Free	62	20	16	26
SUDAN	Not Free	63	17	19	27
UNITED ARAB EMIRATES	Not Free	66	13	22	31
BELARUS	Not Free	67	16	22	29
PAKISTAN	Not Free	67	20	20	27
SAUDI ARABIA	Not Free	70	14	24	32
BAHRAIN	Not Free	72	11	26	35
VIETNAM	Not Free	75	14	28	33
UZBEKISTAN	Not Free	78	20	28	30
ETHIOPIA	Not Free	79	22	28	29
SYRIA	Not Free	85	24	25	36
CHINA (PRC)	Not Free	86	19	29	38
CUBA	Not Free	86	24	29	33
IRAN	Not Free	91	22	32	37

CHARTS AND GRAPHS OF KEY FINDINGS

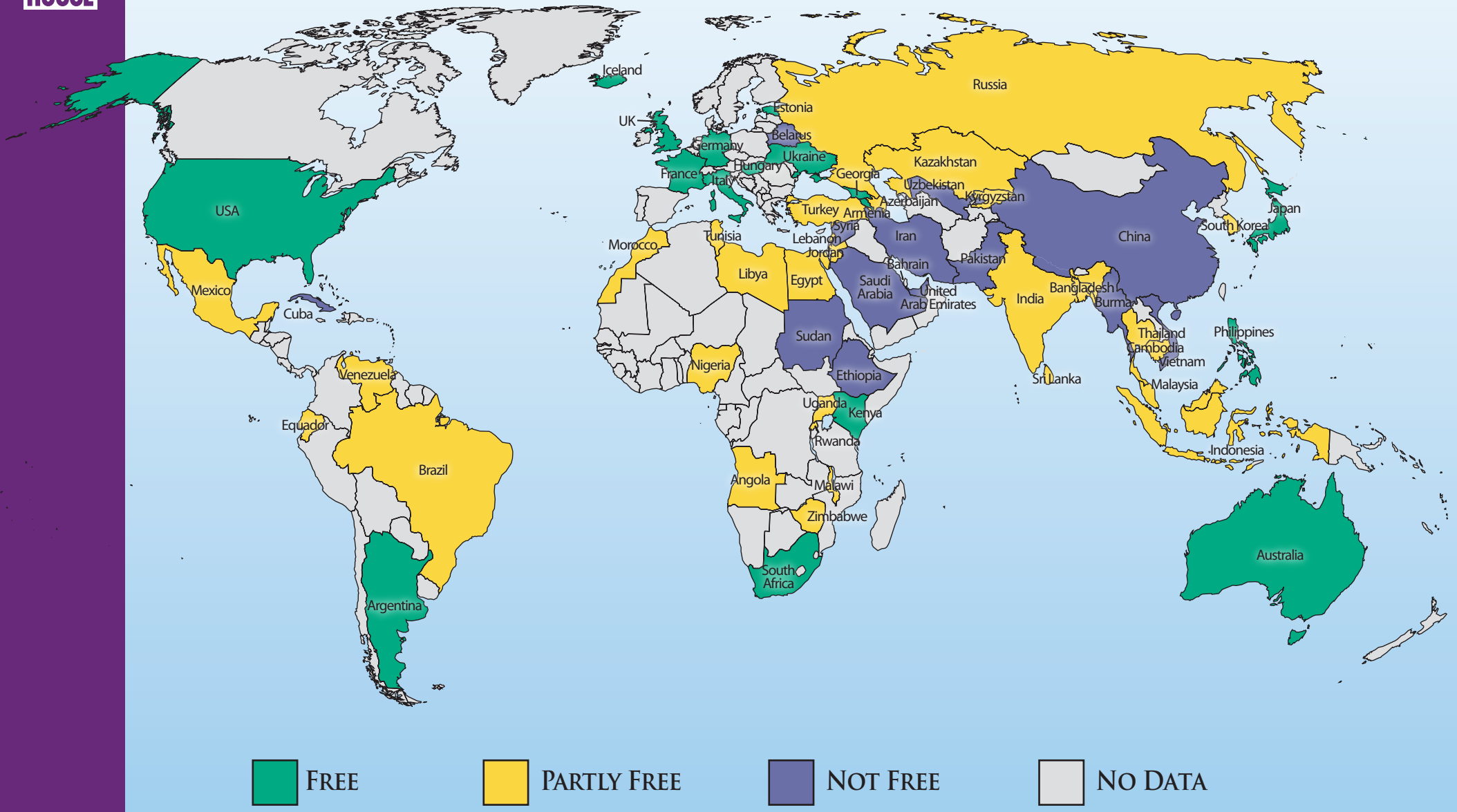
60 COUNTRY SCORE COMPARISON (0 = Most Free, 100 = Least Free)



CHARTS AND GRAPHS OF KEY FINDINGS

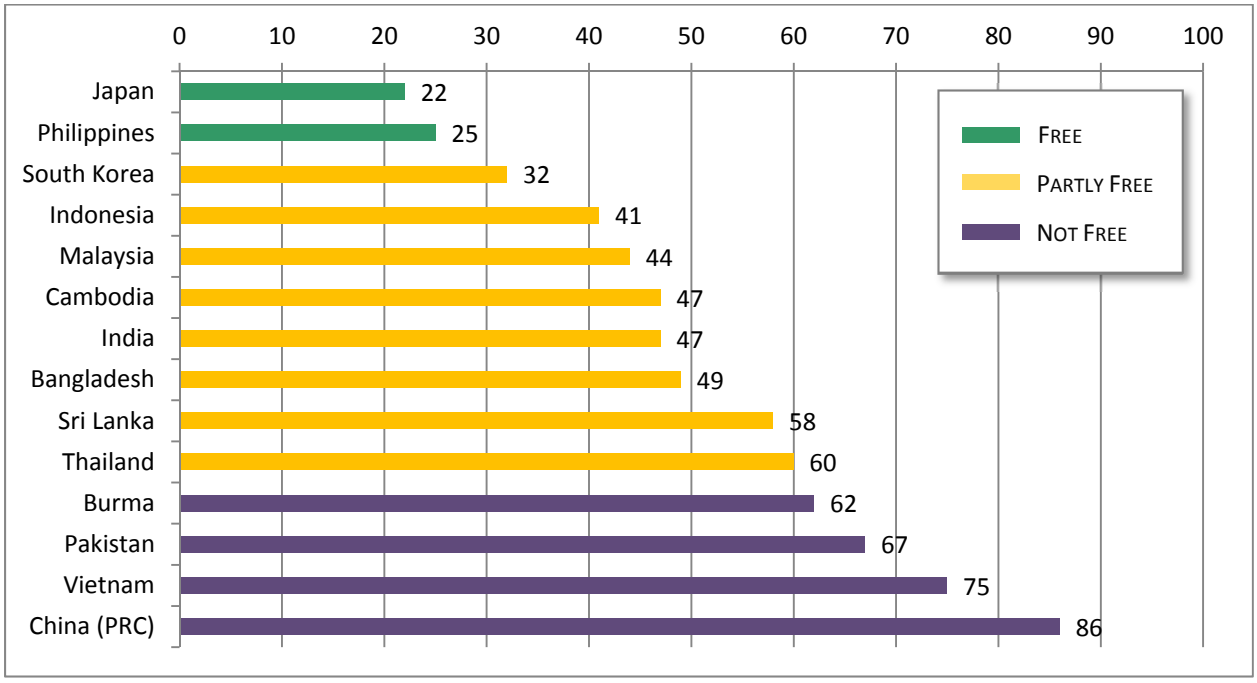
Freedom on the Net 2013

A Global Assessment of Internet and Digital Media

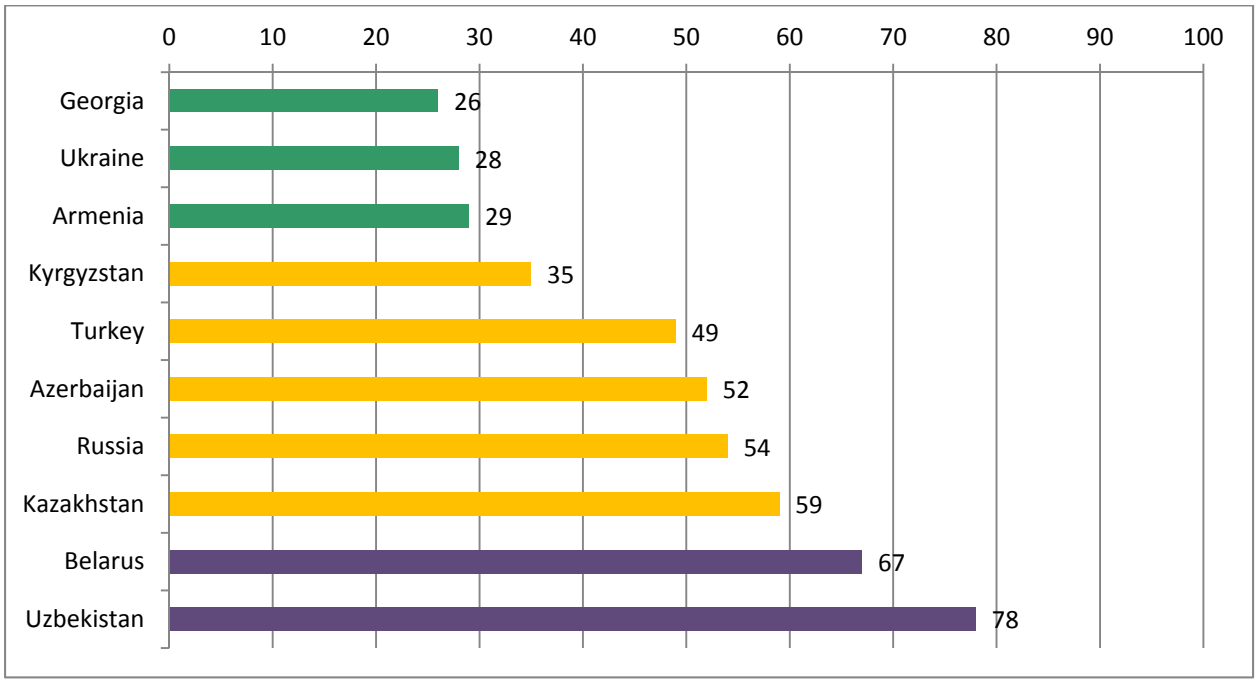


REGIONAL GRAPHS

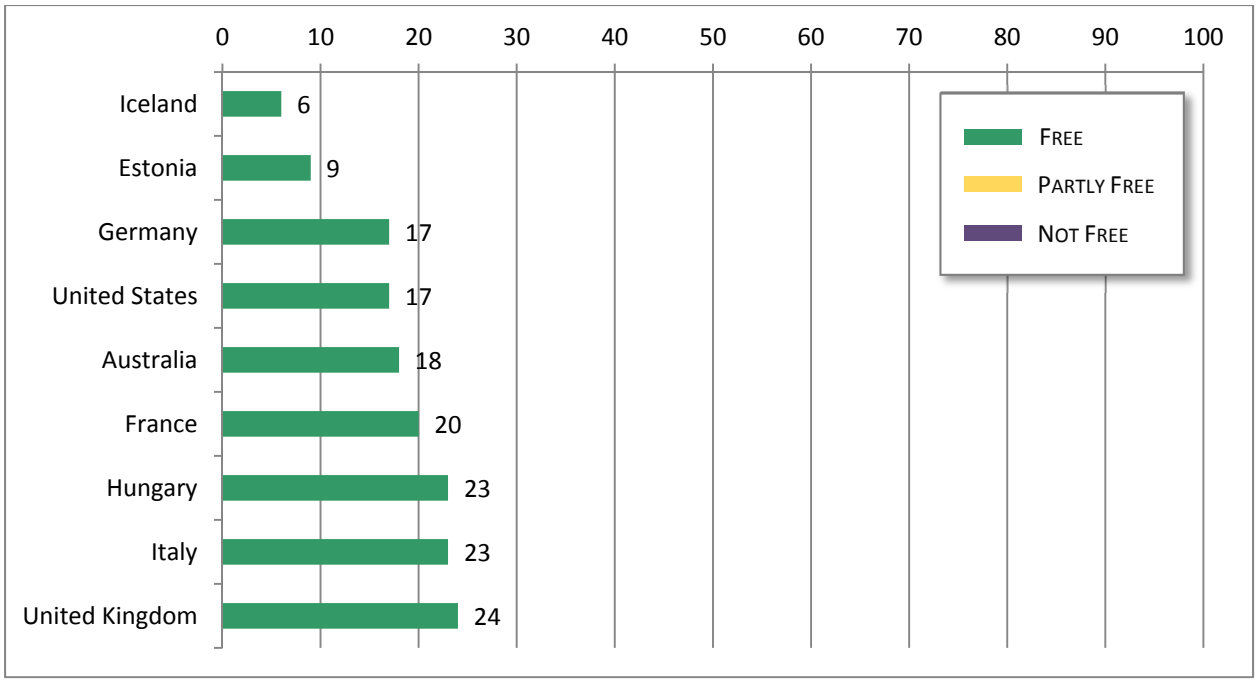
ASIA (0 = Most Free, 100 = Least Free)



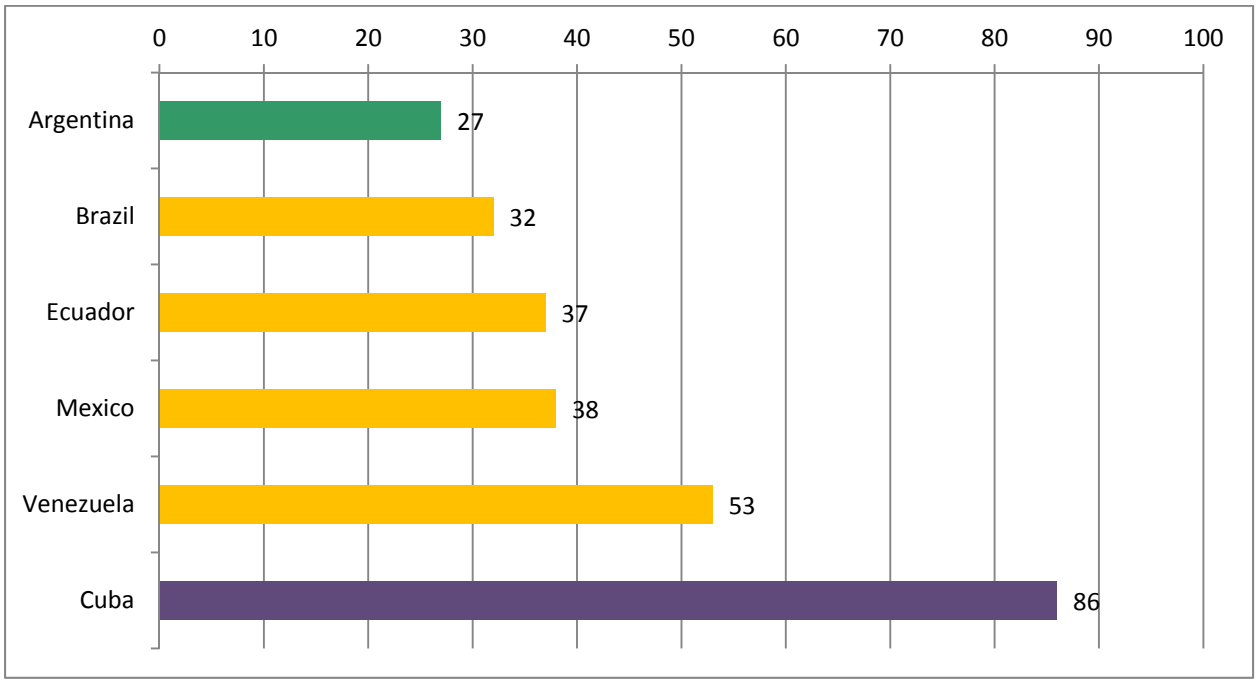
EURASIA (0 = Most Free, 100 = Least Free)



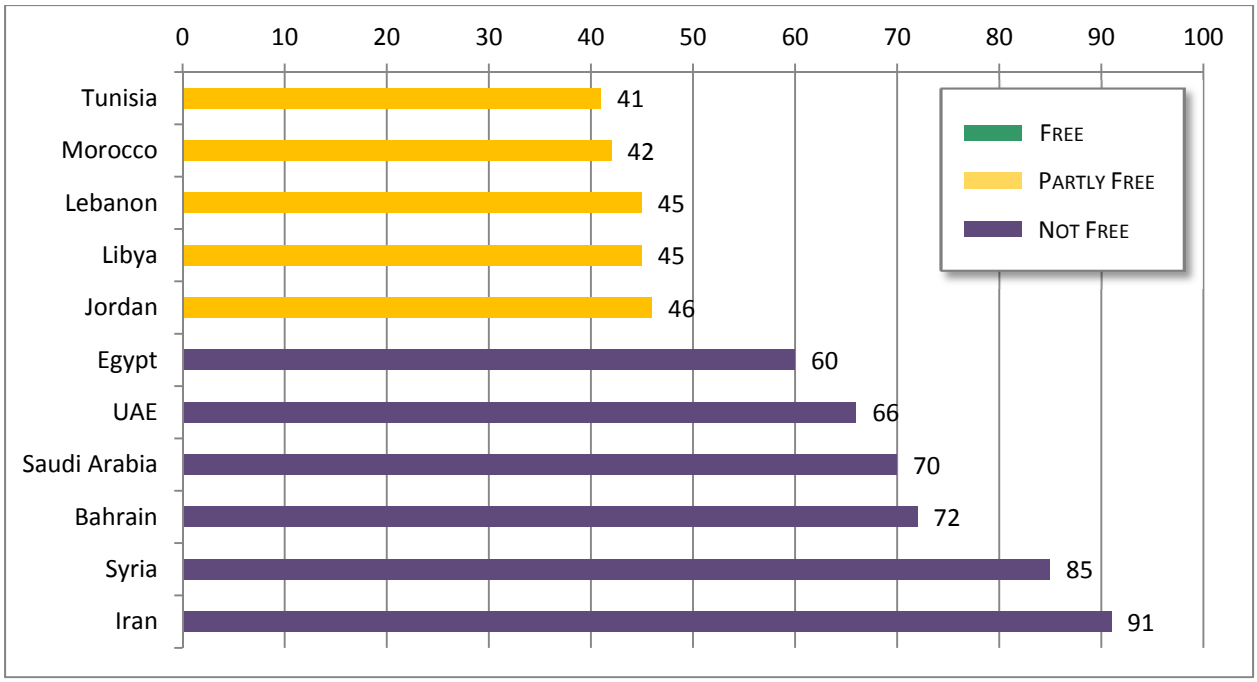
AUSTRALIA , EU, ICELAND & UNITED STATES (0 = Most Free, 100 = Least Free)



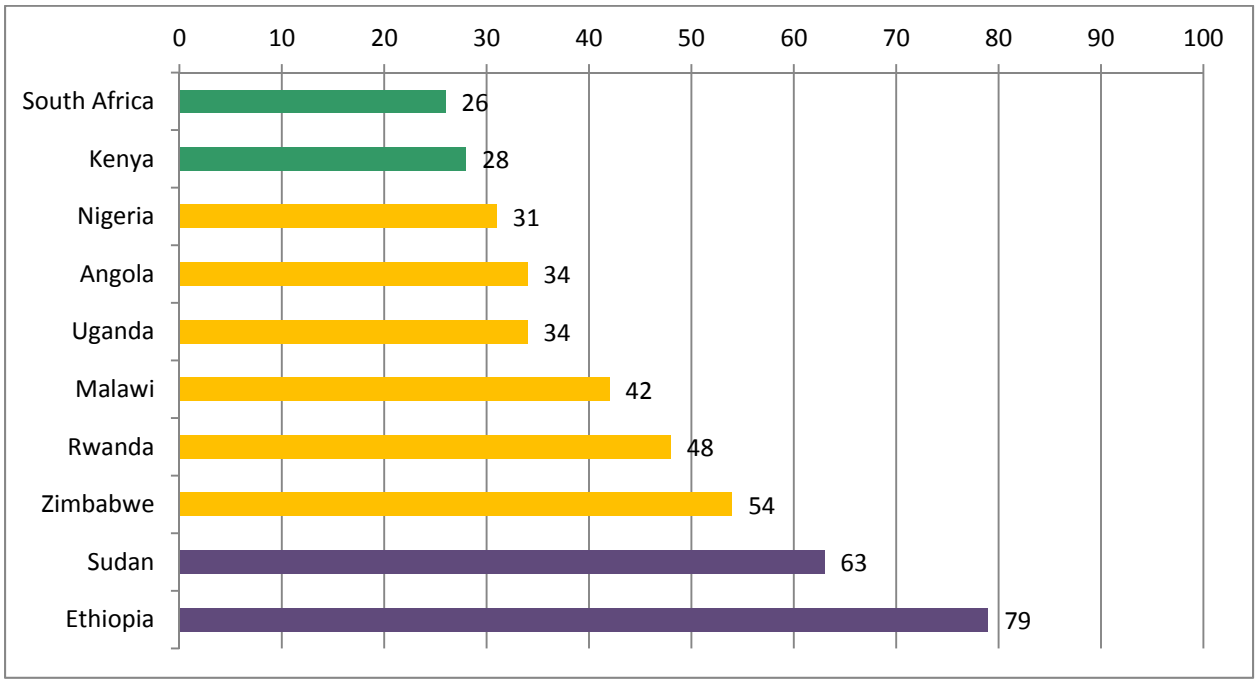
LATIN AMERICA (0 = Most Free, 100 = Least Free)



MIDDLE EAST & NORTH AFRICA (0 = Most Free, 100 = Least Free)

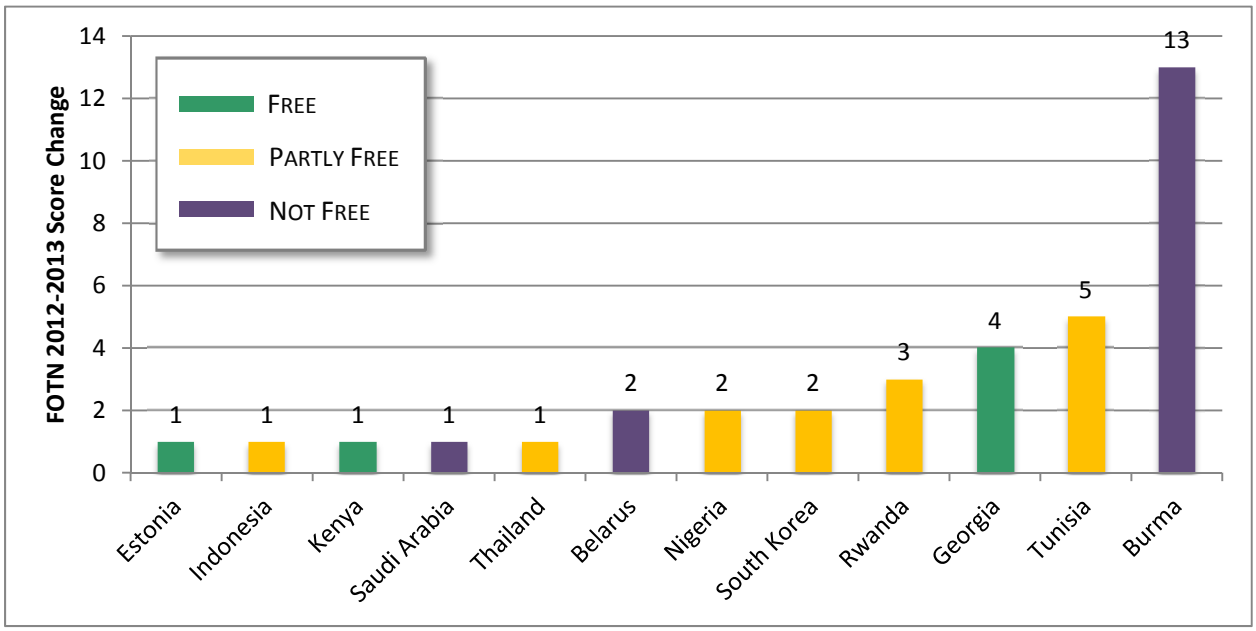


SUB-SAHARAN AFRICA (0 = Most Free, 100 = Least Free)



SCORE CHANGES: FREEDOM ON THE NET 2012 VS. 2013

SCORE IMPROVEMENTS



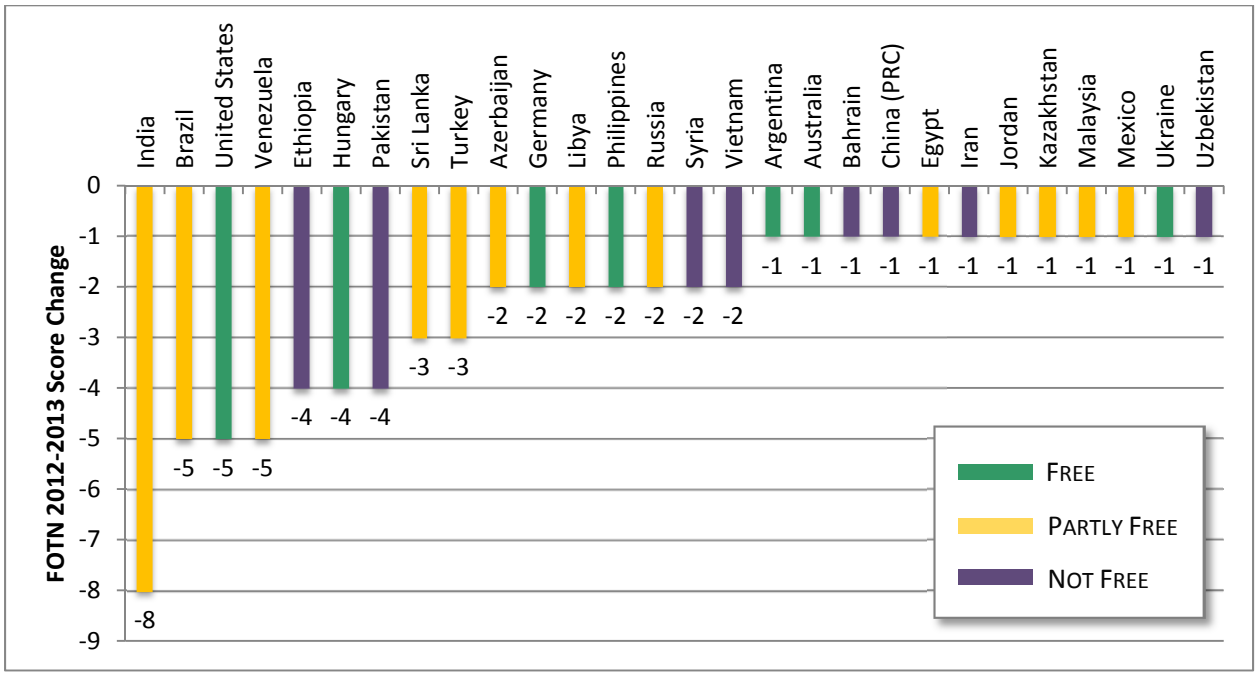
Twelve countries registered positive score changes between the 2012 and 2013 editions of *Freedom on the Net*. In some countries—such as Tunisia and Burma—the improvements reflect government efforts to open up the online sphere. In several countries, however, the improvements registered mainly because of a decrease in the number of negative incidents from the previous coverage period, at times because the authorities had less need to utilize certain types of internet control.

COUNTRY	FOTN 2012	FOTN 2013	TRAJECTORY*
Estonia	10	9	Slight ↑
Indonesia	42	41	Slight ↑
Kenya	29	28	Slight ↑
Saudi Arabia	71	70	Slight ↑
Thailand	61	60	Slight ↑
Belarus	69	67	Slight ↑

COUNTRY	FOTN 2012	FOTN 2013	TRAJECTORY*
Nigeria	33	31	Slight ↑
South Korea	34	32	Slight ↑
Rwanda	51	48	Notable ↑
Georgia	30	26	Notable ↑
Tunisia	46	41	Significant ↑
Burma	75	62	Significant ↑

*A *Freedom on the Net* score decrease represents a positive trajectory (↑) for internet freedom.

SCORE DECLINES



COUNTRY	FOTN 2012	FOTN 2013	TRAJECTORY*
India	39	47	Significant ↓
Brazil	27	32	Significant ↓
United States	12	17	Significant ↓
Venezuela	48	53	Significant ↓
Ethiopia	75	79	Notable ↓
Hungary	19	23	Notable ↓
Pakistan	63	67	Notable ↓
Sri Lanka	55	58	Notable ↓
Turkey	46	49	Notable ↓
Azerbaijan	50	52	Slight ↓
Germany	15	17	Slight ↓
Libya	43	45	Slight ↓
Philippines	23	25	Slight ↓
Russia	52	54	Slight ↓

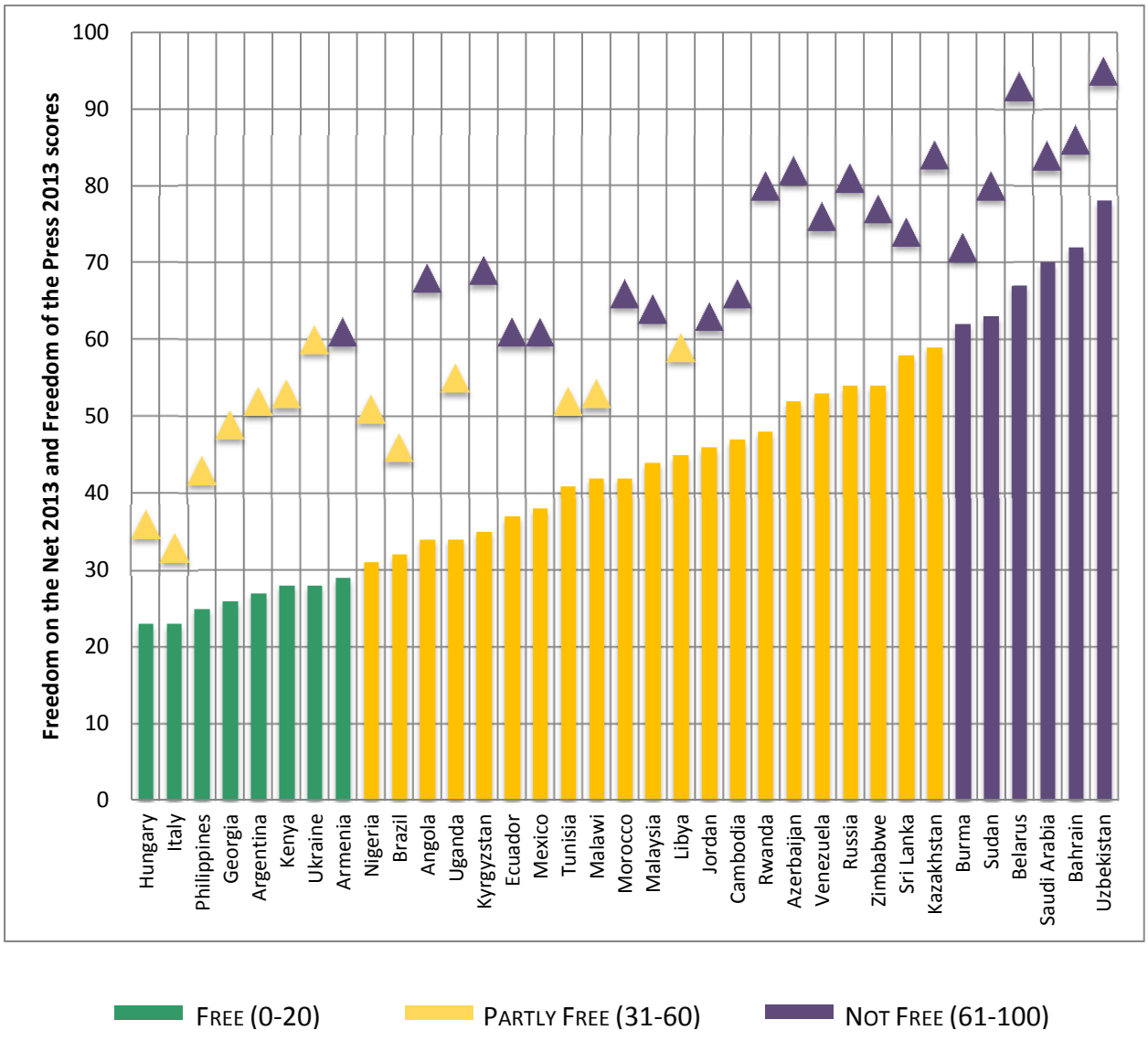
COUNTRY	FOTN 2012	FOTN 2013	TRAJECTORY*
Syria	83	85	Slight ↓
Vietnam	73	75	Slight ↓
Argentina	26	27	Slight ↓
Australia	17	18	Slight ↓
Bahrain	71	72	Slight ↓
China (PRC)	85	86	Slight ↓
Egypt	59	60	Slight ↓
Iran	90	91	Slight ↓
Jordan	45	46	Slight ↓
Kazakhstan	58	59	Slight ↓
Malaysia	43	44	Slight ↓
Mexico	37	38	Slight ↓
Ukraine	27	28	Slight ↓
Uzbekistan	77	78	Slight ↓

*A *Freedom on the Net* score increase represents a negative trajectory (↓) for internet freedom.

INTERNET FREEDOM VS. PRESS FREEDOM

Digital media in several of the 60 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 2013* and *Freedom of the Press 2013* assessments.

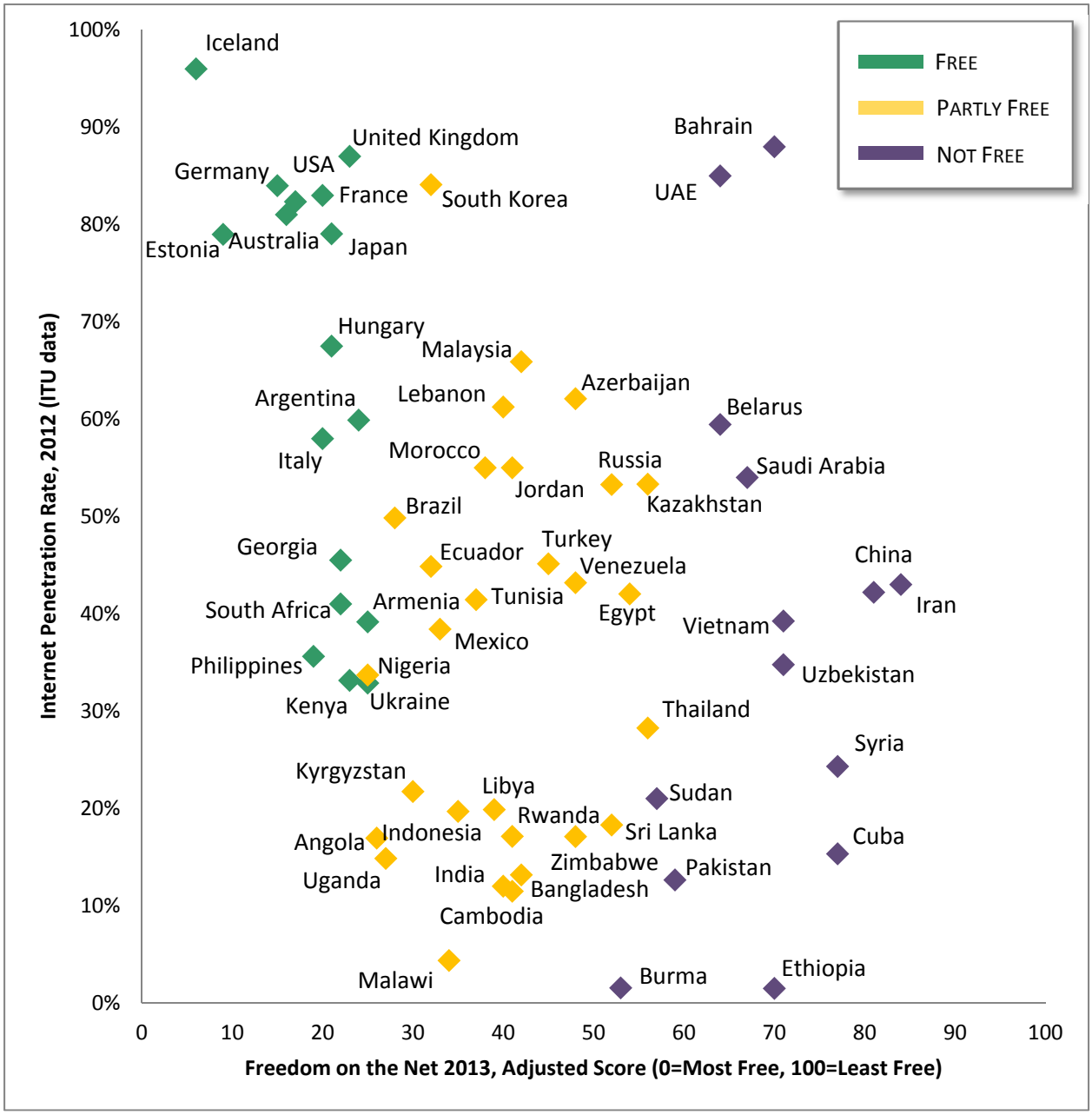
The figure below shows the 35 countries in this edition with a score difference of 10 points or greater. The bar graph characterizes a country's *Freedom on the Net 2013* score, while the scatterplot (▲) represents the country's score in *Freedom of the Press 2013*, which measures media freedom in the 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.



INTERNET FREEDOM VS. INTERNET PENETRATION

The figure below depicts the relationship between internet penetration rates and the level of digital media freedom in *Freedom on the Net 2013*. 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.



METHODOLOGY

This fourth edition of *Freedom on the Net* provides analytical reports and numerical ratings for 60 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, 2012 and April 30, 2013.

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 via 3G networks or satellite?*
   - *Is there a significant difference between internet and mobile-phone penetration and access in rural versus urban areas or across other geographical divisions?*
   - *To what extent are broadband services widely available in addition to dial-up?*

2. **Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)**
   - *In countries where the state sets the price of internet access, is it prohibitively high?*
   - *Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?*
   - *Do low literacy rates (linguistic and "computer 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 (i.e. YouTube, Facebook, Skype, 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 (e.g. bureaucratic "red tape") for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?*
- *Does the state place prohibitively high fees on the establishment and operation of access providers?*

5. **To what extent do national regulatory bodies overseeing digital technology operate in a free, fair, and independent manner? (0-4 points)**

- *Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?*
- *Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' interests?*

- *Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?*
- *Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?*
- *Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?*

B. LIMITS ON CONTENT (0–35 POINTS)

1. **To what extent does the state or other actors block or filter internet and other ICT content, particularly on political and social issues? (0-6 points)**

   - *Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?*
   - *Is there significant filtering of text messages or other content transmitted via mobile phones?*
   - *Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of e-mail 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, e-mail 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 tools for mobilization, particularly regarding political and social issues? (0-6 points)

- *To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or the behavior of other powerful societal actors?*
- *To what extent are online communication tools (e.g. Twitter) or social networking sites (e.g. Facebook, Orkut) used as a means to organize politically, including for "real-life" activities?*
- *Are mobile phones and other ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?*

C. VIOLATIONS OF USER RIGHTS (0-40 POINTS)

1. To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)

- *Does the constitution contain language that provides for freedom of speech and of the press generally?*
- *Are there laws or legal decisions that specifically protect online modes of expression?*
- *Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?*
- *Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?*

- *Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?*

2. Are there laws which call for criminal penalties or civil liability for online and ICT activities? (0-4 points)

- *Are there specific laws criminalizing online expression and activity such as posting or downloading information, sending an e-mail, or text message, etc.? (Note: this excludes legislation addressing harmful content such as child pornography or activities such as malicious hacking)*
- *Do laws restrict the type of material that can be communicated in online expression or via text messages, such as communications about ethnic or religious issues, national security, or other sensitive topics?*
- *Are restrictions of internet freedom closely defined, narrowly circumscribed, and proportional to the legitimate aim?*
- *Are vaguely worded penal codes or security laws applied to internet-related or ICT activities?*
- *Are there penalties for libeling officials or the state in online content?*
- *Can an online outlet based in another country be sued if its content can be accessed from within the country (i.e. "libel tourism")?*

3. Are individuals detained, prosecuted or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs, particularly on political and social issues? (0-6 points)

- *Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?*
- *Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via e-mail 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 e-mail 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. cyber espionage, data gathering, DoS 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 non-state actors from within the country's borders) and are they enforced?*

ACKNOWLEDGMENTS

Completion of the *Freedom on the Net* publication would not have been possible without the tireless efforts of the following individuals.

As project director, Sanja Kelly oversaw the research, editorial, and administrative operations, supported by research analysts Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz, and senior research assistant Ashley Greco-Stoner. Together, they provided essential research and analysis, edited the country reports, conducted field visits in Uganda, Indonesia, Mexico, Jordan, and Hungary, and led capacity building workshops abroad. Over 70 external consultants served as report authors and advisors, and made an outstanding contribution by producing informed analyses of a highly diverse group of countries and complex set of issues.

Helpful contributions and insights were also made by Daniel Calingaert, executive vice president; Arch Puddington, vice president for research; as well as other Freedom House staff in the United States and abroad. Freedom House is also grateful to Cristiana Gonzalez and Eleonora Rabinovich for their contributions during the Latin America ratings review meeting.

This publication was made possible by the generous support of the Dutch Ministry of Foreign Affairs, U.S. State Department's Bureau of Democracy, Human Rights, and Labor (DRL), and Google. The content of the publication is the sole responsibility of Freedom House and does not necessarily reflect the views of the Dutch Foreign Ministry, DRL, Google, or any other funder.

CONTRIBUTORS

FREEDOM HOUSE RESEARCH TEAM

- Sanja Kelly, Project Director, Freedom on the Net
- Mai Truong, Research Analyst (Africa) and Staff Editor, 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; Atilio Grimani, Research Assistant, CELE
- **Australia:** Dr. Alana Maurushat, Senior Lecturer, University of New South Wales
- **Azerbaijan:** Arzu Geybullayeva, Analyst
- **Bangladesh:** Faheem Hussain, Assistant Professor of ICT and Computer Science, Asian University for Women
- **Brazil:** Carolina Rossini, Project Director, Latin America Resource Center, New America Foundation
- **Burma:** Min Zin, Ph.D. Candidate, Department of Political Science, University of California, Berkeley and Contributor, *Foreign Policy* Transitions blog
- **Cambodia:** Sopheap Chak, Program Director of the Cambodian Center for Human Rights and Blogger
- **China:** Madeline Earp, Research Analyst, Freedom on the Net, Freedom House
- **Cuba:** Ernesto Hernández Busto, Cuban journalist and writer based in Barcelona, Spain
- **Ecuador:** Carlos Correa Loyola, Co-Founder, Asociación de Usuarios Digitales
- **Estonia:** Linnar Viik, Associate Professor, Estonian IT College
- **France:** Jean-Loup Richet, Researcher, University of Nantes
- **Georgia:** Giga Paitchadze, Blogger
- **Germany:** Dr. Jeanette Hofmann, Research Director at the Alexander von Humboldt Institute for Internet and Society, Berlin and Researcher at the Social Science Research Center, Berlin;

Christian Katzenbach, Project Coordinator, and Kirsten Gollatz, Project Manager, Alexander von Humboldt Institute for Internet and Society

- **Hungary:** Borbála Tóth, Independent Researcher; Sandor Orban, Program Director, South East European Network for Professionalization of Media
- **Iceland:** Caroline Nellemann, Independent Consultant and Specialist in Digital Media and Civic Engagement
- **Indonesia:** Enda Nasution, Co-Founder, Sebangsa.com
- **Iran:** Mahmood Enayat, Director, Small Media
- **Italy:** Giampiero Giacomello, Assistant Professor of International Relations, University of Bologna
- **Japan:** Izumi Aizu, Professor and Senior Research Fellow, Institute for InfoSocionomics, Tama University, Tokyo and Executive Director, Institute for HyperNetwork Society, Oita
- **Jordan:** Abeer al-Najjar, Assistant Professor of Journalism and Media Studies, American University of Sharjah
- **Kazakhstan**: Adil Nurmakov, Founder of the "Basta" Citizen Initiative and Editor of the Blogbasta.kz website
- **Kenya:** Grace Githaiga, Kenya ICT Action Network (KICTANet)
- **Kyrgyzstan:** Tattu Mambetalieva, Director, Civil Initiative on Internet Policy (CIIP); Artem Goriyanov, IT Programs Director, CIIP
- **Lebanon:** Dr. Jad Melki, Assistant Professor of Journalism and Media Studies and Director, Media Studies Program, American University of Beirut
- **Malawi:** Vitus-Gregory Gondwe, Senior Reporter for Blantyre Newspapers Limited, Specialist Writer on ICT News for BizTechAfrica.com and Bizcommunity.com
- **Malaysia:** K. Kabilan, Chief Editor, FMTNews.com
- **Mexico:** Alejandra Ezeta, Social Media Consultant at EEB Consultaoria/Ciudadanos en Medios, A.C., Mexico
- **Morocco:** Bouziane Zaid, Assistant Professor of Media and Communication, Al Akhawayn University in Ifrane
- **Nigeria:** 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria
- **Pakistan:** Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan, Lawyer, and Internet Freedom Activist
- **Philippines:** Jacques DM Gimeno, Assistant Professor, Communication Research Department, University of the Philippines-Diliman
- **South Africa:** Alex Comninos, Doctoral Candidate, Justus Liebig University Giessen
- **South Korea:** Yenn Lee, Research Skills Coordinator, School of Oriental and Africa Studies, University of London
- **Sri Lanka:** Nigel V. Nugawela, Independent Writer and Researcher
- **Sudan:** GIRIFNA, a Sudanese non-violent resistance movement
- **Syria:** Mohammad al-Abdallah, Syrian Human Rights Activist and Independent Researcher

- **Thailand:** Sawatree Suksri, Lecturer in Criminal Law and Criminal Procedural Law, Thammasat University, Bangkok
- **Turkey:** Yaman Akdeniz, Professor of Law, Istanbul Bilgi University and Founder of Cyber-Rights.org
- **Uganda:** Peter Mwesige, Executive Director, African Centre for Media Excellence (ACME); Grace Natabaalo, Program Associate, ACME; and Ashnah M. Kalemera, Program Officer, Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
- **Ukraine:** Tetyana Lokot, Doctoral Student and Researcher at the Philip Merrill College of Journalism, University of Maryland, College Park
- **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, Postdoctoral Research Fellow, University Researcher Priority Program Asia and Europe, University of Zurich (at time of writing)
- **Zimbabwe:** Rashweat Mukundu, Journalist, Media and Freedom of Expression Activist, Zimbabwe

The analysts for the reports on Armenia, Bahrain, Belarus, Egypt, Ethiopia, Libya, Russia, Rwanda, Saudi Arabia, Tunisia, the United Arab Emirates, Venezuela, and Vietnam are independent internet researchers who have requested to remain anonymous. Freedom House researchers Madeline Earp, Mai Truong, and Ashley Greco-Stoner provided analysis for the India, Angola, and Ecuador reports, respectively, in consultation with a range of in-country stakeholders. Xiao Qiang, Director of the China Internet Project at the University of California, Berkeley, was an advisor for the China report.

ABOUT FREEDOM HOUSE

Freedom House is an independent private organization supporting the expansion of freedom throughout the world.

Freedom is possible only in democratic political systems in which governments are accountable to their own people, the rule of law prevails, and freedoms of expression, association, and belief are guaranteed. Working directly with courageous men and women around the world to support nonviolent civic initiatives in societies where freedom is threatened, Freedom House functions as a catalyst for change through its unique mix of analysis, advocacy, and action.

- **Analysis:** Freedom House's rigorous research methodology has earned the organization a reputation as the leading source of information on the state of freedom around the globe. Since 1972, Freedom House has published *Freedom in the World*, an annual survey of political rights and civil liberties experienced in every country of the world. The survey is complemented by an annual review of press freedom, an analysis of transitions in the post-communist world, and other publications.
- **Advocacy:** Freedom House seeks to encourage American policymakers, as well as other government and international institutions, to adopt policies that advance human rights and democracy around the world. Freedom House has been instrumental in the founding of the worldwide Community of Democracies, has actively campaigned for a reformed Human Rights Council at the United Nations, and presses the Millennium Challenge Corporation to adhere to high standards of eligibility for recipient countries.
- **Action:** Through exchanges, grants, and technical assistance, Freedom House provides training and support to human rights defenders, civil society organizations, and members of the media in order to strengthen indigenous reform efforts in countries around the globe.

Founded in 1941 by Eleanor Roosevelt, Wendell Willkie, and other Americans concerned with mounting threats to peace and democracy, Freedom House has long been a vigorous proponent of democratic values and a steadfast opponent of dictatorships of the far left and the far right. The organization's diverse Board of Trustees is composed of a bipartisan mix of business and labor leaders, former senior government officials, scholars, and journalists who agree that the promotion of democracy and human rights abroad is vital to America's interests.

1301 Connecticut Avenue, NW; Washington, DC 20036
(202) 296-5101

120 Wall Street, New York; NY 10025
(212) 514-8040

1301 Connecticut Avenue, NW; Washington, DC 20036
(202) 296-5101

120 Wall Street, New York; NY 10025
(212) 514-8040