Privatizing Censorship, Eroding Privacy

October 2015

Freedom House

FREEDOM ON THE NET 2015

Freedom on the Net 2015

Table of Contents

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

This booklet is a summary of findings for the 2015 edition of *Freedom on the Net*. A full volume with 65 country reports assessed in this year's study can be found on our website at **www.freedomhouse.org**.

ON THE COVER

Protesters gather to demonstrate against internet censorship in China, one of the partner countries of the CeBit computer trade fair held in Hanover, Germany (March 2015).

Cover image by Alexander Koerner/Getty Images

Freedom House

Privatizing Censorship, Eroding Privacy

by Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong

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

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

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

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

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

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

In more repressive settings where the potential for legislative change is limited, activists have had some success in using information and communication

In September 2015, the Chinese government censored images of the cartoon character Winnie the Pooh, which internet users on the microblogging site Sina Weibo posted in an allusion to the image of President Xi Jinping in a military parade. The image was shared over 65,000 times before it was removed and became the most censored image on Sina Weibo that month.

Getty Images

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

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

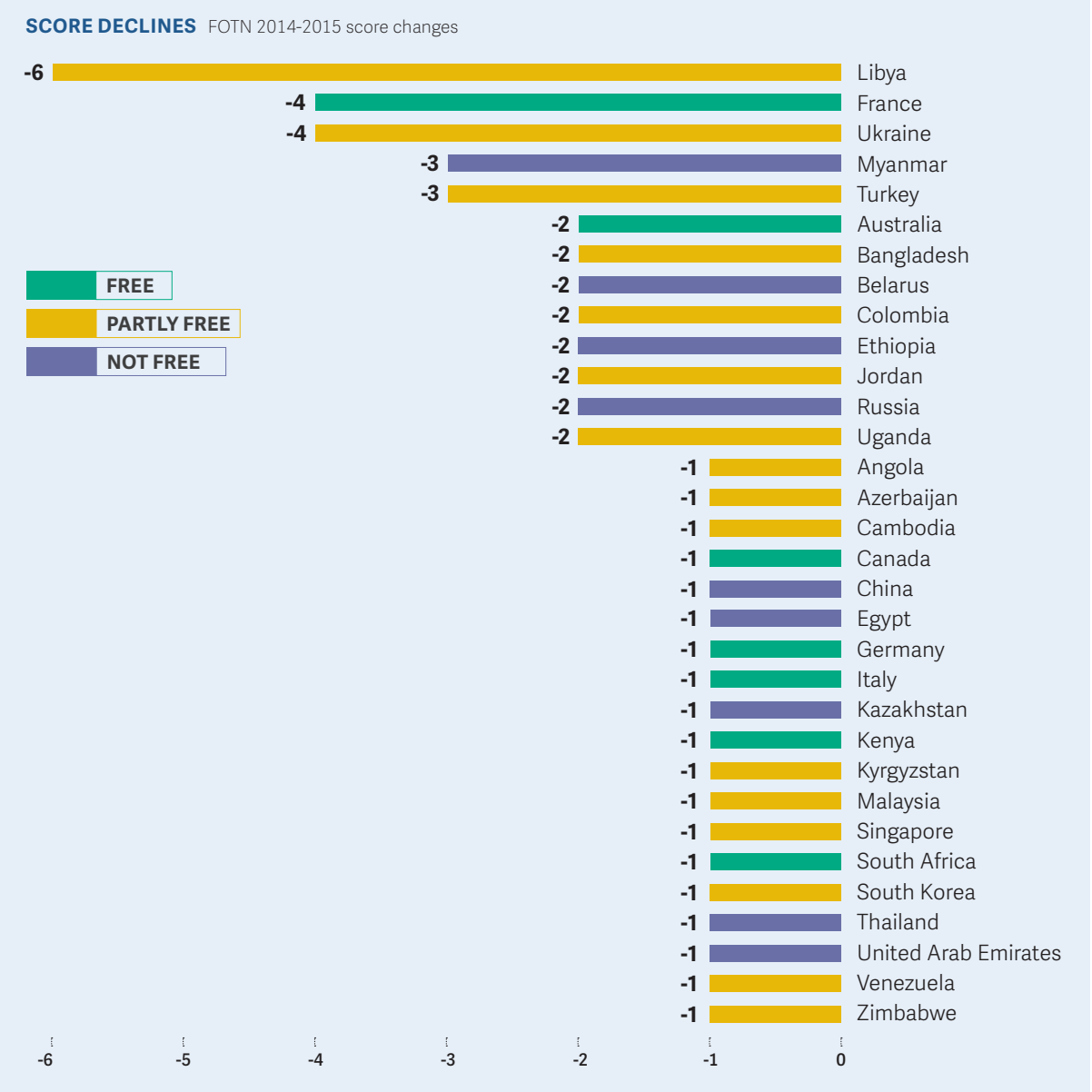
While the overall trajectory for internet freedom remains negative, the declines over the last year were less precipitous than in the past. The small victories described above are promising signs that the setbacks of recent years can be reversed, and that the fight for a free and open internet will continue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

Tracking the Global Decline

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

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

China was the year's worst abuser of internet freedom. As President Xi Jinping made "cyber sovereignty" one of the priorities of his tenure as leader of the Chinese Communist Party, internet users endured crackdowns on "rumors," greater enforcement of rules against anonymity, and disruptions to the circumvention tools that are commonly used to bypass censorship. Though not entirely new, these measures were implemented with unprecedented intensity. Google, whose services were frequently interrupted in the past, was almost completely blocked. Veteran human rights defenders were jailed for online expression, including lawyer Pu Zhiqiang, who faces charges of "picking quarrels" in connection with 28 social media posts, and 70-year-old journalist Gao Yu, who was sentenced to seven years in prison for sending "state secrets" to a foreign website. Official censorship directives during the year suppressed online commen-



tary on issues ranging from Hong Kong prodemocracy protests to stock-market volatility.

Syria and Iran were the second- and third-worst performers, respectively. Activists, bloggers, and citizen journalists in Syria continue to risk death at the hands of armed factions from across the political spectrum. In Iran, positive moves by President Hassan Rouhani and the ICT Ministry have led to greater bandwidth and the expansion of 3G services across all major networks. However, despite the president's reformist rhetoric, major improvements to civil liberties remain blocked by the supreme leader and the country's conservative establishment. Eight young people were sentenced to a combined 127 years in prison for anti-government posts on Facebook in July 2014.

By contrast, 15 countries registered overall improvements. The year's biggest gains occurred in Sri Lanka following the January 2015 elections. The new government unblocked previously inaccessible websites and ceased harassing and prosecuting internet users. Cuba also registered an improvement after the reestablishment of diplomatic relations with the United States, marking a potential opening for the ICT sector. The cost of public internet access, though still out of reach for most Cubans, was cut in half; the first public Wi-Fi connections were established; and online media began to adopt a more critical tone toward the authorities. And Zambia enjoyed a reduction in major restrictions on online content compared with the previous year—a trend that continued under the new government elected in January 2015.

Frequently Censored Topics

The following is a selection of the topics that were subject to censorship in the 65 countries covered in *Freedom on the Net*. A country was deemed to censor a topic if it blocked relevant webpages, initiated takedown and deletion requests, or detained users who posted content on that topic.

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

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

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

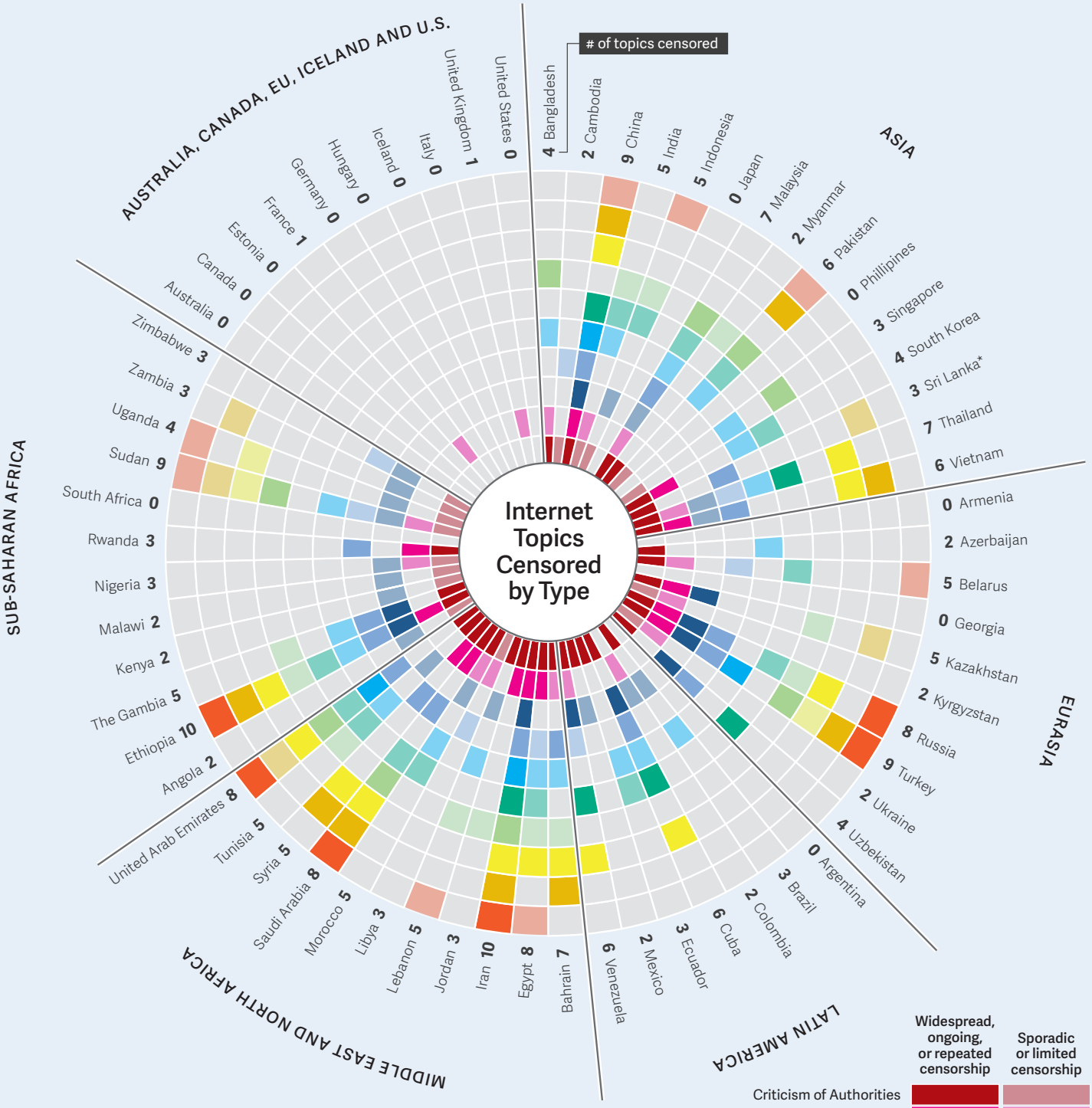
Satire: Authorities in 23 of the 65 countries assessed went to great lengths to muzzle ridicule and ironic commentary about public officials. A court in Bangladesh, for example, sentenced a 25-year-old to seven years in prison—the minimum under the amended ICT Act—for sharing a satirical song via his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

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

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

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

LGBTI Issues: Fourteen countries targeted LGBTI (lesbian, gay, bisexual, transgender, and intersex) content for censorship on moral, religious, or other



Methods represented here are usually explicitly state-sanctioned, including blocking, content removal, and prosecutions. The chart does not consider extralegal pressures like violence, self-censorship, or cyberattacks, even where the state is believed to be responsible.

* Until Jan. 2015

grounds, reflecting the entrenched and often state-endorsed bias against the LGBTI community in some parts of the world. Lebanon blocked a lesbian forum used throughout the Arab region, and a transgender woman in Egypt was sentenced to six years in prison over YouTube videos that showed her dancing.

Ethnic and Religious Minorities: Thirteen countries censored information by or about a minority community, reinforcing routine discrimination against marginalized groups and obstructing efforts to combat it. In Vietnam, content promoting organized Buddhism, Roman Catholicism, and the Cao Dai religious group was blocked, while the UAE blocked an online forum for Arab Christians.

Conflict: News and opinion on conflict, terrorism, or outbreaks of violence were subject to censorship in 29 of the 65 countries reviewed. In Jordan, the owner and the editor in chief of the Saraya News website were held on charges of spreading false news and aiding a terrorist organization for their coverage of the kidnapping of Jordanian pilot Moath al-Kasasbeh by IS militants in 2014. In China, a 22-year-old Uighur man was detained for "rumor mongering" in online posts about civilian deaths during 2014 clashes in Xinjiang.

Major Trends

With Blocking Less Effective, States Push for Content Removal

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

More governments are now pressuring companies and individuals to remove content, as opposed to simply blocking.

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

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

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

The trend is apparent not just in the number of governments taking this approach, but also in the num-

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

Incentives Driving the Trend

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

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

Technology Companies' Predicament

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

Common Content-Removal Methods

- **Content removal requests:** Requests may come from government agencies, but also from individuals, businesses, or other entities, preferably with a court order. Depending on the company and platform, these may be subject to an internal review by the company that considers the merit of each request. In some cases, however, content is removed without much scrutiny to avoid penalties mandated by law, particularly when it is hosted within the jurisdiction that initiated the request.
- **Proactive policing by intermediaries:** Laws that hold service providers, content hosts, or webmasters disproportionately liable for third-party (user) content can motivate these intermediaries to proactively police the content on their platforms and remove anything that may result in legal penalties. This is different from purely voluntary action taken by some intermediaries to monitor their services and enforce their own policies on issues like violence or obscenity.
- **Coerced deletions:** Individual users, news sites, or other content producers can be directly pressured to delete content, for example through phone calls, arrests, and interrogations.

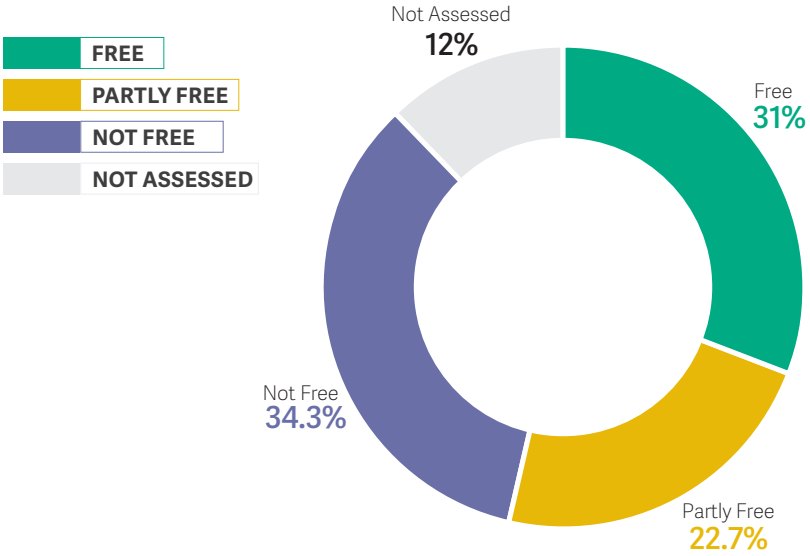
However, many governments go much further in shifting the burden of censorship, forcing private companies to proactively monitor their networks and err on the side of caution to comply with vaguely worded regulations. Of the 65 countries assessed in *Freedom on the Net*, 26 hold intermediaries liable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

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

In the best cases involving censorship requests, companies act as a positive check on the repressive inten-

GLOBAL INTERNET POPULATION BY 2015 FOTN STATUS

FOTN assesses 88 percent of the world's internet users.



tions of weak governments. They closely scrutinize government demands against local laws and refuse to comply if the requests do not meet basic legal standards. Frequently, though, these firms have to choose between free-speech considerations and the survival of their business in the country.

Coercion of Individuals

In some instances, instead of turning to tech companies, authoritarian governments have gone directly to individual content creators and coerced them into deleting material through intimidation or torture. This method is particularly appealing to governments when the targeted content is hosted abroad, meaning requests to foreign companies might take more time and resources, and could ultimately be denied.

Governments in 14 of 65 countries passed new laws to increase surveillance over the past year.

In Bahrain, for example, after the arrest of the user allegedly behind the satirical Twitter account @Takrooz, almost 100,000 tweets were deleted. Only one tweet remained on the account at the time of writing: "They tortured me in prison." In Saudi Arabia, sentences for posting controversial content online often include requirements to close social media accounts and bans on further posts. When the human rights lawyer Walid Abulkhair refused, his prison sentence was increased from 10 to 15 years.

Surveillance Laws and Technologies on the Rise

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

Laws Expose User Data

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

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

This trend is even more concerning in countries where internet freedom violations occur more frequently. After the Russian government issued a decree in April

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

Surveillance Technologies Proliferate

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

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

Governments Target Encryption, Anonymity

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

Stigmatizing Encryption

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

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

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

Encryption has been stigmatized as a tool for terrorists, contributing to illegitimate arrests. In August 2015, three staff members working for Vice News were arrested in southeastern Turkey and charged with supporting terrorists after authorities found encryption software on one of their computers. Similar accusations were brought against three Al-Jazeera journalists who were detained in Egypt and the Zone 9 bloggers in Ethiopia.

Undermining Anonymity

While encryption protects the content of communications, anonymity is necessary for securing the privacy of users' metadata. Tools such as virtual private networks (VPNs), proxies, and Tor can disguise an individual's original internet protocol (IP) address and other details that would reveal the identity or location of users. However, governments around the globe are working to restrict these methods, undermining international norms on user anonymity. Belarus, Ethiopia, Indonesia, Iran, Kazakhstan, and Uzbekistan are among the countries that have ordered bans on Tor, or circumvention tools more broadly, and China blocked access to several popular VPNs in the past year.

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

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

Arrests and Intimidation of Users Escalate

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

Prison Sentences

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

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

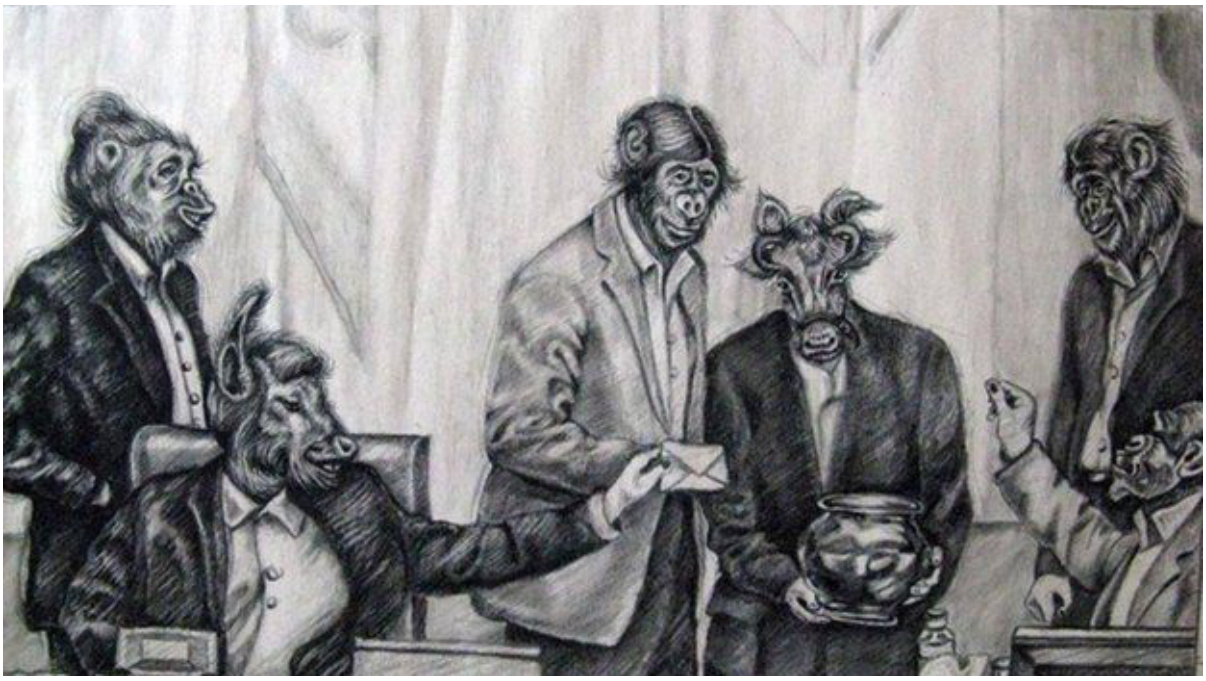
Violence and Harassment

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

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

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

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



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

ist. They posted explicit photos of Shchyrakova that were apparently taken from a computer confiscated by the state security service in 2010.

Youth Targeted

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

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

Emerging Issues

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

Net Neutrality

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

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

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

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

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

The 'Right to Be Forgotten'

In May 2014, the Court of Justice of the European Union granted individuals the right to request that search engines hide links to public information about them if it is no longer accurate or relevant, establishing their "right to be forgotten." However, aside from information about public figures, the ruling provided little guidance as to what types of information should

be hidden or retained in the public interest, meaning search engines would have to decide on a case-by-case basis, in an internal process that lacks the oversight and transparency of established legal proceedings.

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

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

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

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

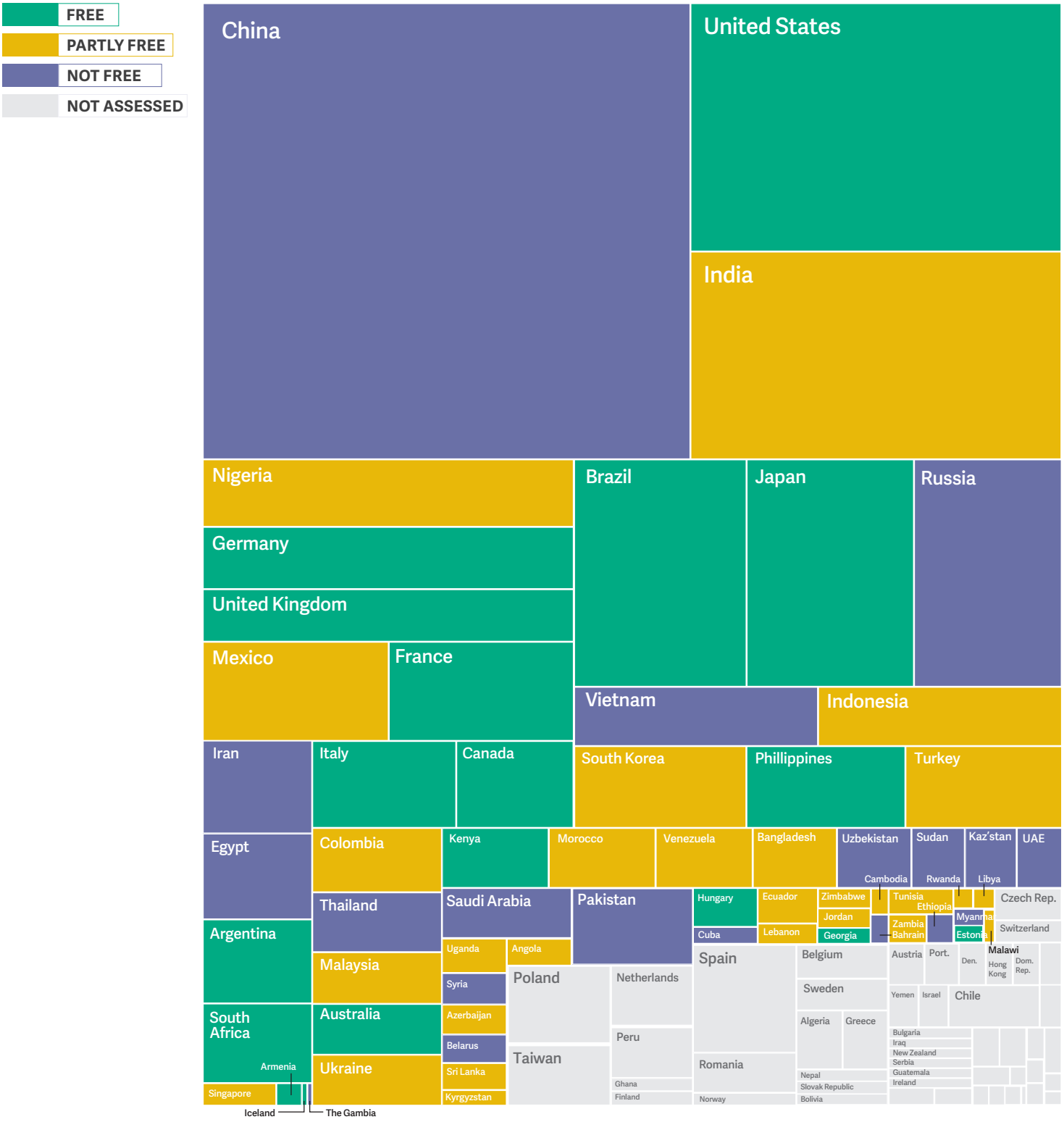
Conclusion

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

It remains to be seen whether repressive efforts will be sustainable in the long run. The global struggle for internet freedom led to several positive achievements over the past year, raising the possibility of greater advances in the future. Digital activism has been and remains a vital driver of change around the world, particularly in societies that lack political rights and press freedom. The greatest gains, however, have been made through legislative changes or judicial decisions, indicating that countries with meaningful political debates and independent judiciaries have a distinct advantage in safeguarding internet freedom over their more authoritarian counterparts. These victories and others like them could help ensure that the fight for a free and open internet ultimately succeeds, despite the setbacks that have affected so much of the world in recent years.

DISTRIBUTION OF GLOBAL INTERNET USERS BY COUNTRY AND FOTN STATUS

The 65 countries covered in *Freedom on the Net* represent 88 percent of the world's internet user population. Over 40 percent of global internet users live in three countries — China, the United States, or India — that span the spectrum of internet freedom environments, from Free to Not Free.



GLOBAL INTERNET USERS

Over **3 billion people** have access to the internet.

According to Freedom House estimates:

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

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

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

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

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

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

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

34% live under governments which **disconnected internet or mobile phone access** in 2014-2015, often for political reasons.

KEY INTERNET CONTROLS BY COUNTRY

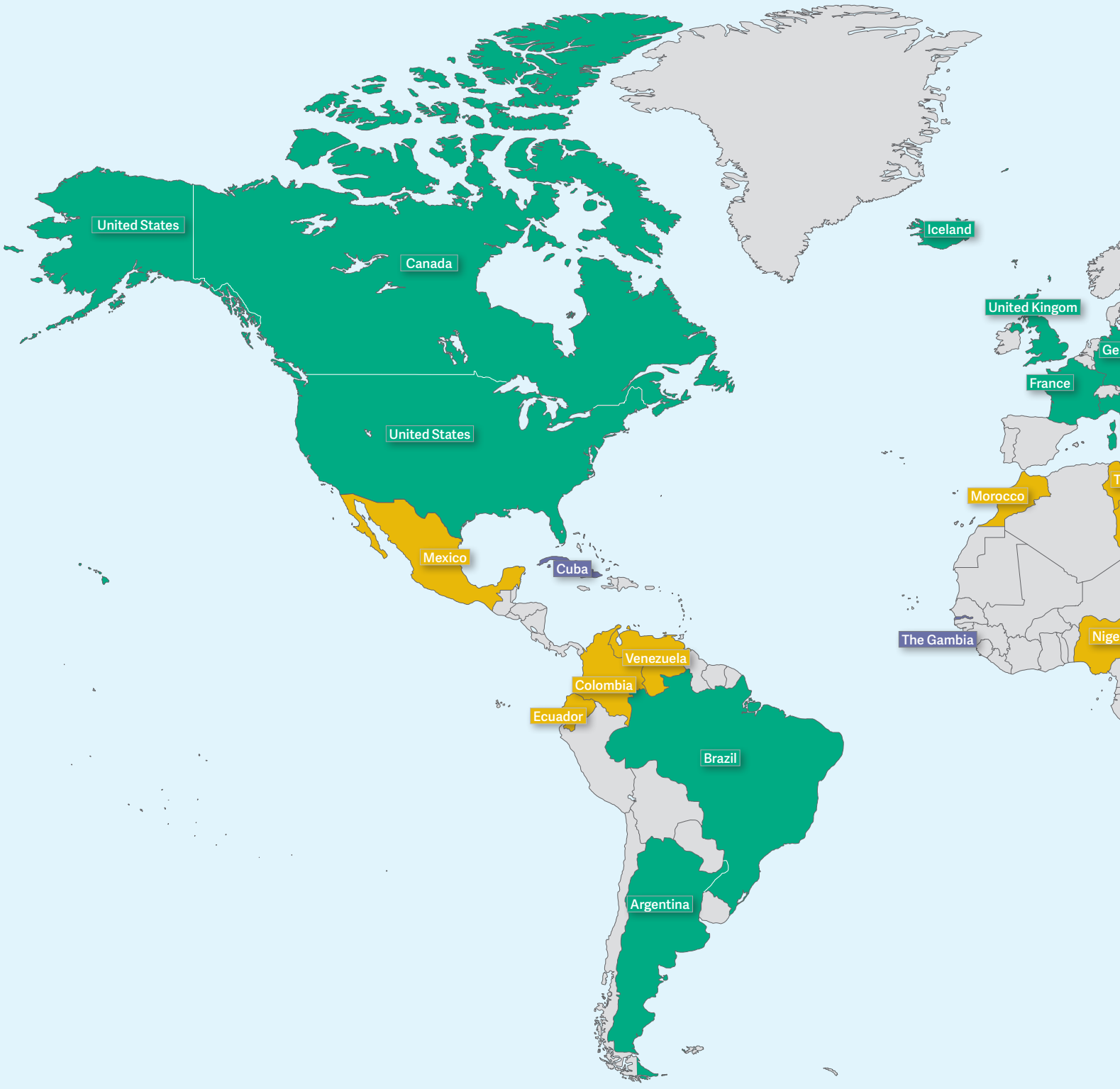
Country (by FOTN 2015 ranking)	"FOTN 2015 score (0=Most Free, 100=Lease Free)"	"FOTN 2015 Status (F=Free, PR=Partly Free, NF=Not Free)"	Social media and/or communications apps blocked	Political, social, and/or religious content blocked	Localized or nationwide ICT shut down	Progovernment commentators manipulate online discussions	New law/directive increasing censorship or punishment passed	New law/directive increasing surveillance or restricting anonymity passed	Online journalist/blogger/ICT user arrested, imprisoned, and/or in prolonged detention for political or social content	Online journalist/blogger/ICT user physically attacked or killed (including while in custody)	Technical attacks against government critics and human rights organizations	"TOTAL # of Key Internet Controls employed in 2014-2015, by country"
Iceland	6	F										0
Estonia	7	F										0
Canada	16	F						●				1
Germany	18	F										0
Australia	19	F						●				1
United States	19	F										0
Japan	22	F										0
Italy	23	F						●				1
France	24	F					●	●	●			3
Georgia	24	F										0
Hungary	24	F										0
United Kingdom	24	F					●	●				2
Argentina	27	F										0
Phillipines	27	F			●							1
South Africa	27	F										0
Armenia	28	F									●	1
Brazil	29	F								●		1
Kenya	29	F						●	●			2
Colombia	32	PF										0
Nigeria	33	PF							●		●	2
South Korea	34	PF		●					●			2
Kyrgyzstan	35	PF		●		●		●				3
Uganda	36	PF							●		●	2
Ecuador	37	PF				●					●	2
Ukraine	37	PF		●					●	●	●	4
Tunisia	38	PF							●		●	2
Angola	39	PF							●		●	2
Mexico	39	PF				●		●	●	●	●	5
India	40	PF	●	●	●				●	●		5
Malawi	40	PF										0
Zambia	40	PF										0
Singapore	41	PF							●			1
Indonesia	42	PF	●	●			●		●			4

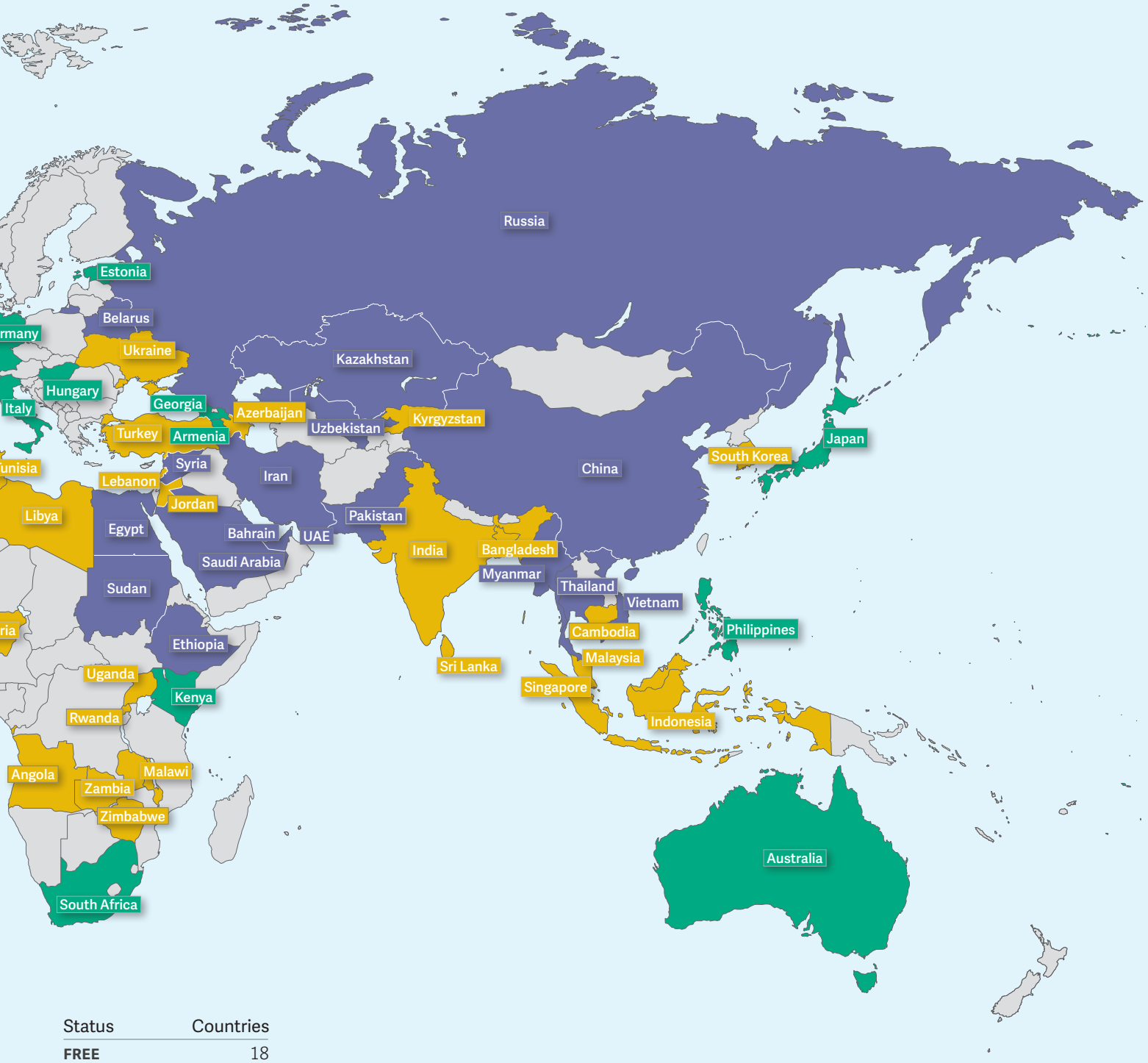
● = Internet control observed during the June 2014 - May 2015 coverage period.
● = Internet control observed after May 31, 2014 until the time of writing.
● = ICT user arrested prior to coverage period but serving part or all of prison sentence during coverage period.

Country (by FOTN 2015 ranking)	"FOTN 2015 score (0=Most Free, 100=Lease Free)"	"FOTN 2015 Status (F=Free, PR=Partly Free, NF=Not Free)"	Social media and/or communications apps blocked	Political, social, and/or religious content blocked	Localized or nationwide ICT shut down	Progovernment commentators manipulate online discussions	New law/directive increasing censorship or punishment passed	New law/directive increasing surveillance or restricting anonymity passed	Online journalist/blogger/ICT user arrested, imprisoned, and/or in prolonged detention for political or social content	Online journalist/blogger/ICT user physically attacked or killed (including while in custody)	Technical attacks against government critics and human rights organizations	"TOTAL # of Key Internet Controls employed in 2014-2015, by country"
Malaysia	43	PF		●		●	●		●			4
Morocco	43	PF				●			●		●	3
Lebanon	45	PF		●					●		●	3
Sri Lanka	47	PF		●								1
Cambodia	48	PF		●								1
Jordan	50	PF		●					●			2
Rwanda	50	PF		●								1
Bangladesh	51	PF	●	●					●	●		4
Libya	54	PF		●	●					●		3
Azerbaijan	56	PF				●	●		●		●	4
Zimbabwe	56	PF						●	●	●	●	4
Venezuela	57	PF		●		●			●		●	4
Turkey	58	PF	●	●		●	●	●	●		●	7
Egypt	61	NF				●	●		●	●	●	5
Kazakhstan	61	NF	●	●	●	●	●		●		●	7
Russia	62	NF		●		●	●		●	●	●	6
Myanmar	63	NF				●			●	●	●	4
Thailand	63	NF		●		●	●	●	●	●		6
Belarus	64	NF		●		●	●	●	●		●	6
The Gambia	65	NF		●					●	●		3
Sudan	65	NF				●	●		●		●	4
United Arab Emirates	68	NF	●	●			●		●			4
Pakistan	69	NF	●	●	●		●		●	●		6
Bahrain	72	NF	●	●		●		●	●		●	6
Saudi Arabia	73	NF	●	●		●			●	●	●	6
Vietnam	76	NF		●		●	●		●	●	●	6
Uzbekistan	78	NF	●	●		●	●		●		●	6
Cuba	81	NF	●	●		●			●	●		5
Ethiopia	82	NF	●	●		●			●	●	●	6
Iran	87	NF	●	●		●			●		●	5
Syria	87	NF	●	●	●	●			●	●	●	7
China	88	NF	●	●	●	●	●	●	●	●	●	9
TOTAL			**15**	**31**	**7**	**24**	**17**	**14**	**40**	**19**	**28**	

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

FREEDOM ON THE NET 2015





Status	Countries
FREE	18
PARTLY FREE	28
NOT FREE	19
Total	**65**

Freedom on the Net 2015 assessed 65 countries around the globe. The project is expected to expand to more countries in the future.

65 COUNTRY SCORE COMPARISON

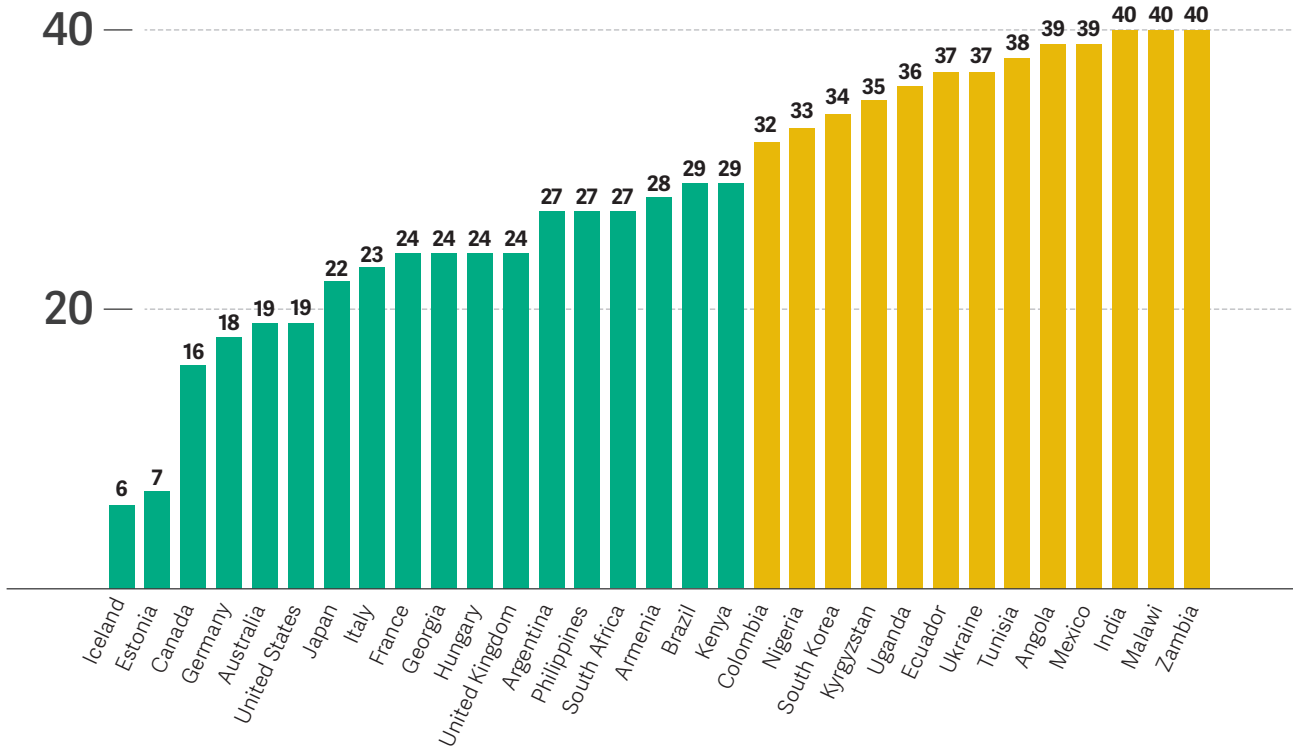
Freedom on the Net measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of FREE (0-30 points), PARTLY FREE (31-60 points), or NOT FREE (61-100 points).

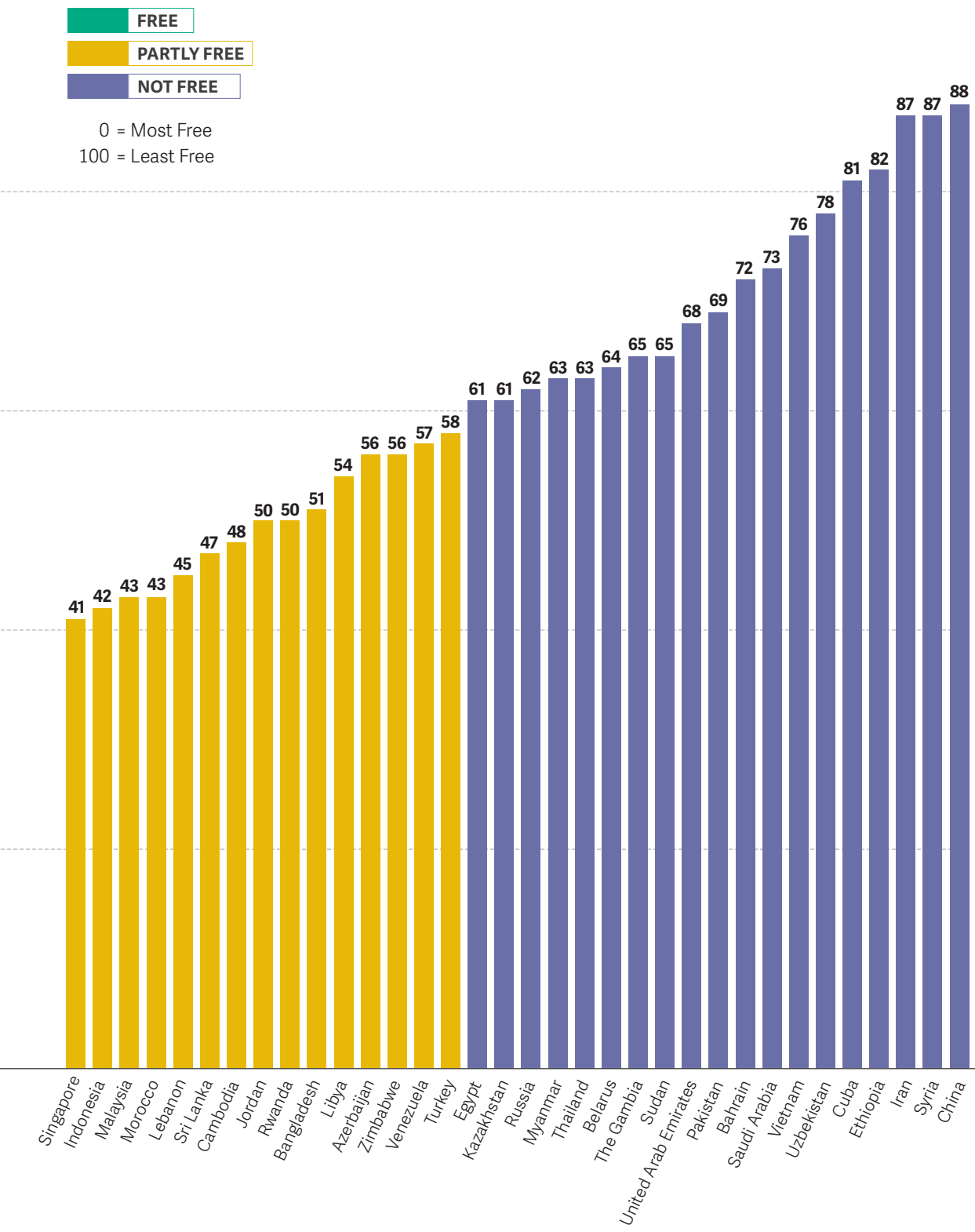
Ratings are determined through an examination of three broad categories:

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

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

C. VIOLATIONS OF USER RIGHTS: Measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.




FREE
PARTLY FREE
NOT FREE
0 = Most Free
100 = Least Free
41
42
43
43
45
47
48
50
50
51
54
56
56
57
58
61
61
62
63
63
64
65
65
68
69
72
73
76
78
81
82
87
87
88
Singapore
Indonesia
Malaysia
Morocco
Lebanon
Sri Lanka
Cambodia
Jordan
Rwanda
Bangladesh
Libya
Azerbaijan
Zimbabwe
Venezuela
Turkey
Egypt
Kazakhstan
Russia
Myanmar
Thailand
Belarus
The Gambia
Sudan
United Arab Emirates
Pakistan
Bahrain
Saudi Arabia
Vietnam
Uzbekistan
Cuba
Ethiopia
Iran
Syria
China

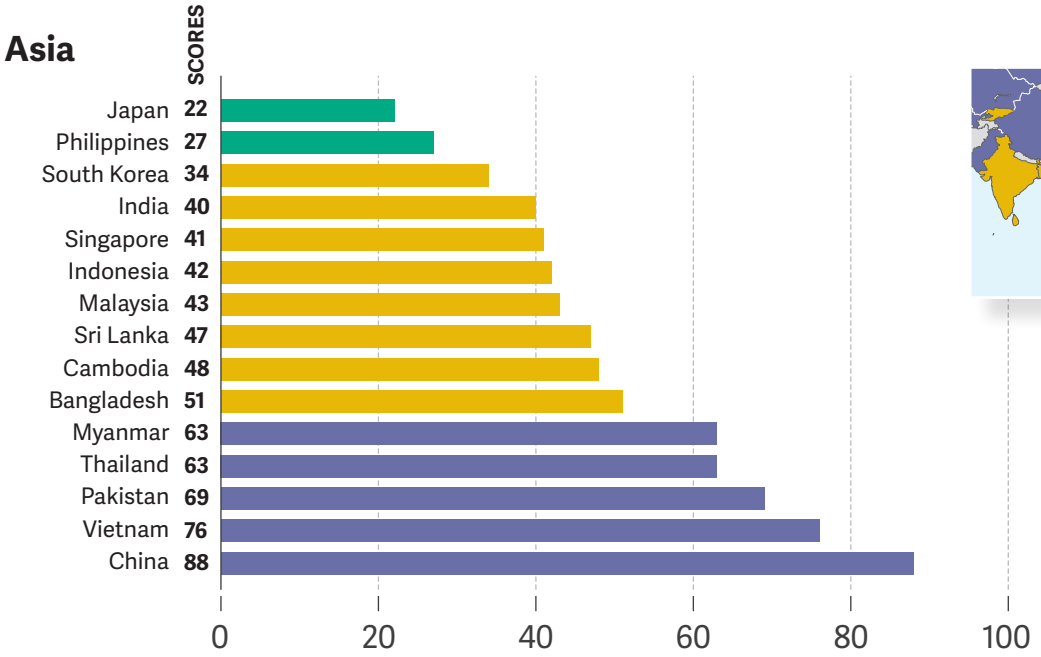
REGIONAL GRAPHS

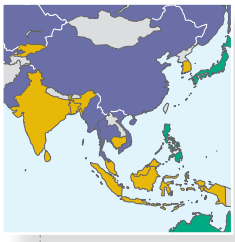
Freedom on the Net 2015 covers 65 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

FREE
PARTLY FREE
NOT FREE

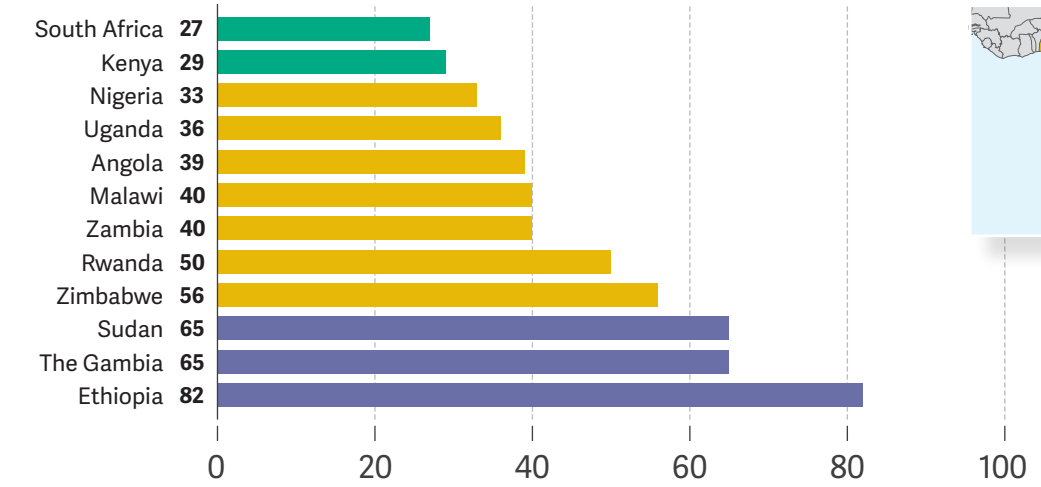
0 = Most Free
100 = Least Free

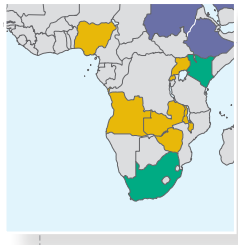
Asia



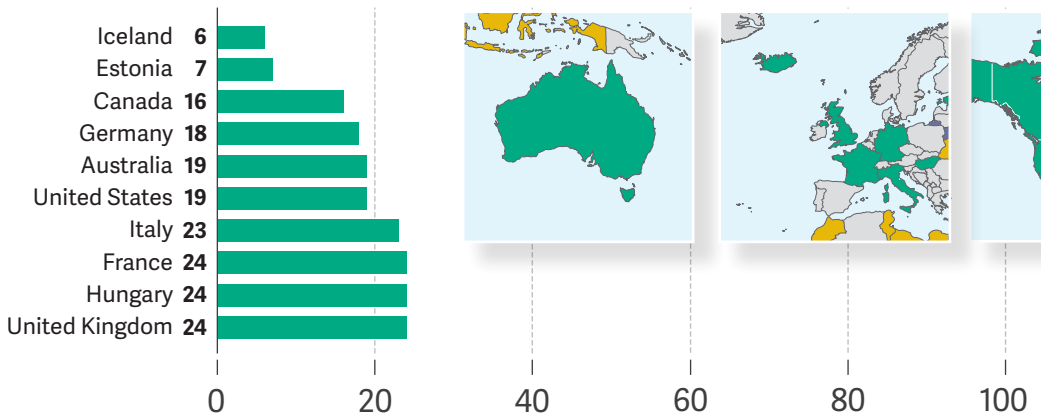


Sub-Saharan Africa

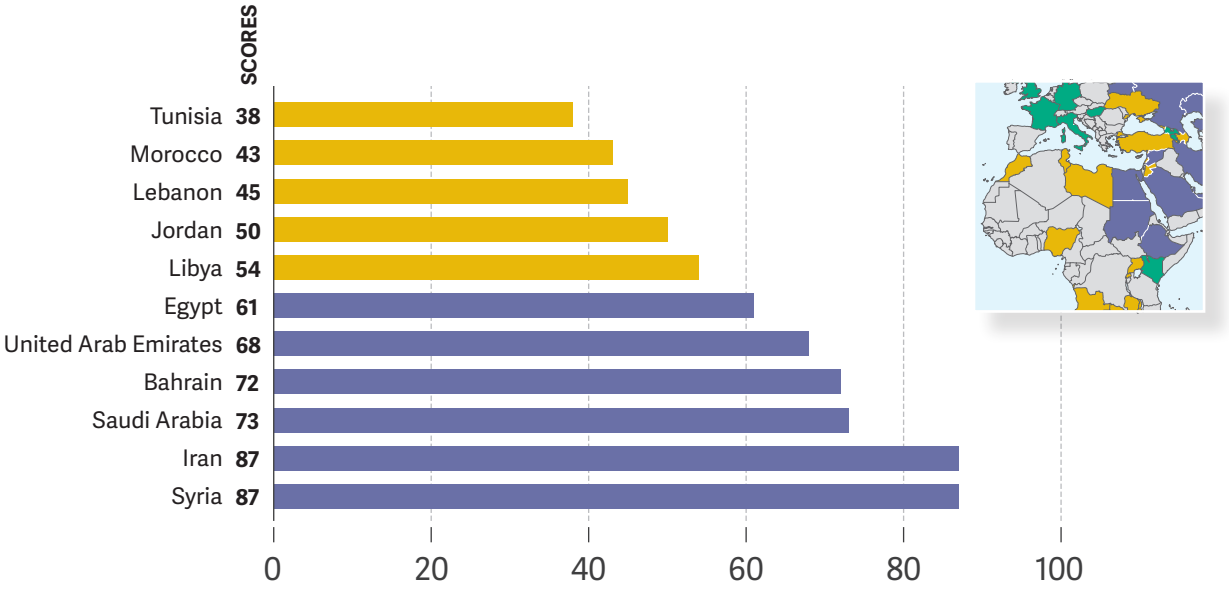




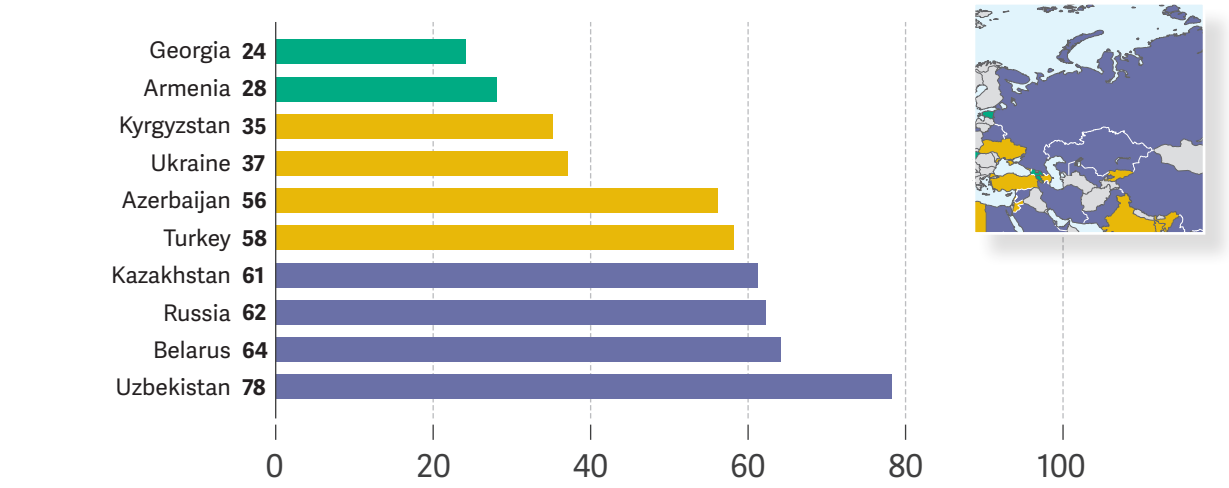
Australia, Canada, European Union, Iceland & United States



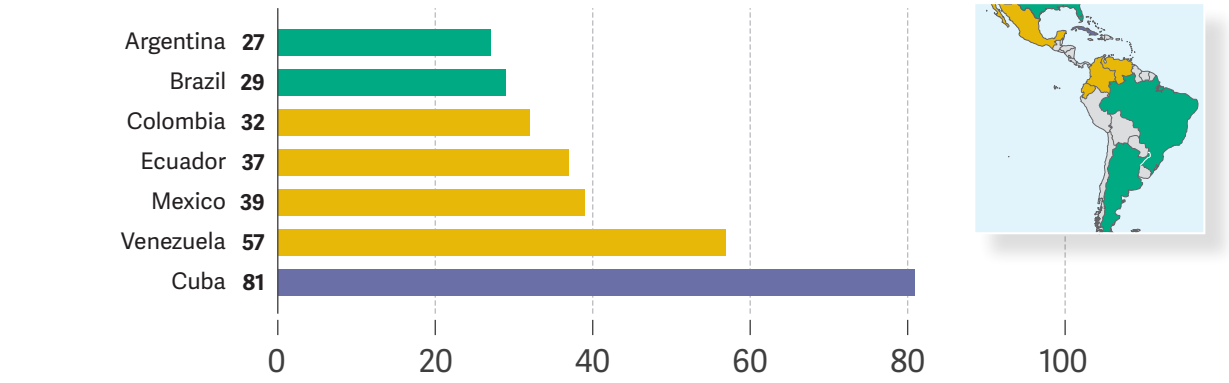
Middle East and North Africa (MENA)



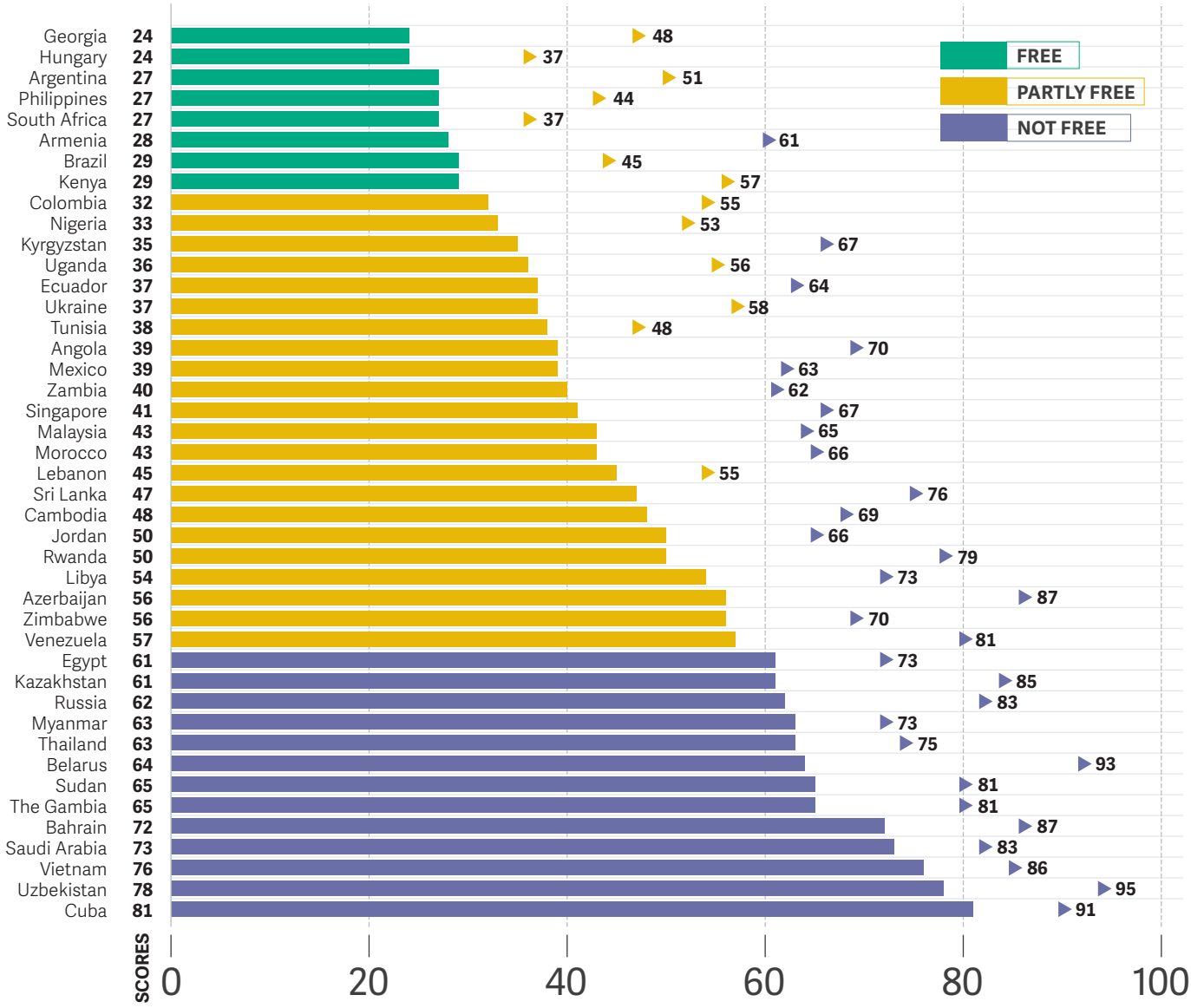
Eurasia



Latin America



INTERNET FREEDOM VS. PRESS FREEDOM

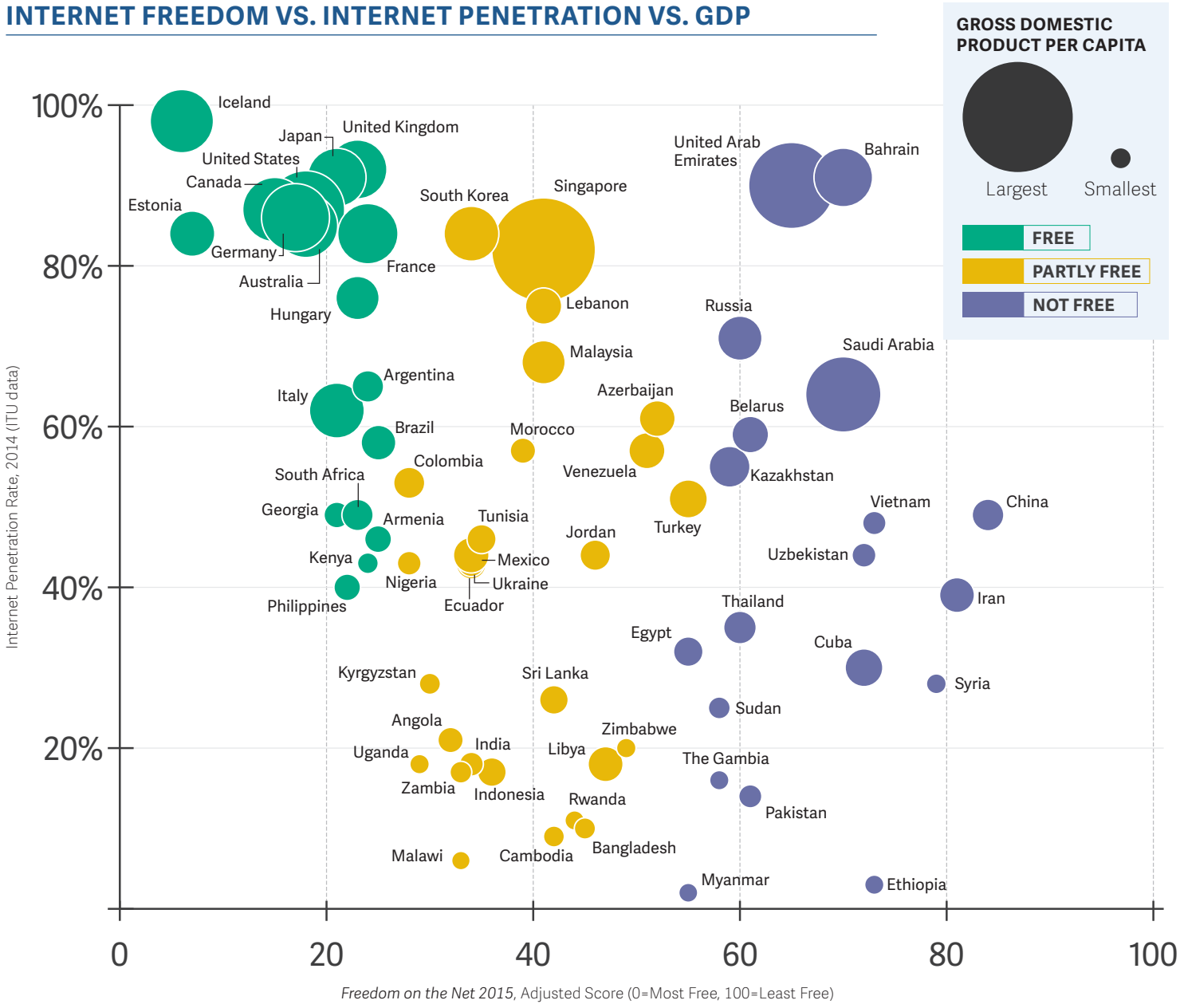


Freedom on the Net 2015 and *Freedom of the Press 2015* scores

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

The figure above shows the 43 countries in this edition with a score difference of 10 points or greater. While pressures that constrain expression in print or broadcast media have the potential to inhibit the online sphere, our data shows that the number of countries with a significantly more free internet environment increased from 37 countries in the last edition, indicating that the internet may be proving more resilient to government control. Nevertheless, attempts by governments to rein in online freedoms remain a cause for concern, particularly in countries that lack press freedom where the internet is often the last remaining outlet for free expression and independent news.

INTERNET FREEDOM VS. INTERNET PENETRATION VS. GDP



The figure above depicts the relationship between internet freedom, internet access, and economic activity as measured by gross domestic product (GDP) per capita data. The x-axis considers a country's score in the 2015 edition of *Freedom on the Net*, adjusted to exclude aspects related to internet access. Levels of internet penetration are plotted against the y-axis, using 2014 statistics from the United Nations International Telecommunication Union (ITU). Finally, the size of each plot is indicative of its GDP per capita (at purchasing power parity, PPP), according to the latest figures from the World Bank.

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

OVERVIEW OF SCORE CHANGES

	Overall				Category Trajectories					
Country	FOTN 2014	FOTN 2015	Overall Trajectory	FOTN 2015 Status	A. Obstacles to Access		B. Limits on Content		C. Violations of User Rights	
Asia										
Bangladesh	49	51	▼	Partly Free	12		12		27	▼
Cambodia	47	48	▼	Partly Free	14		15		19	▼
China	87	88	▼	Not Free	18	▲	30	▼	40	▼
India	42	40	▲	Partly Free	12	▲	10		18	▲
Indonesia	42	42		Partly Free	11		12		19	
Japan	22	22		Free	4		7		11	
Malaysia	42	43	▼	Partly Free	8		14		21	▼
Myanmar	60	63	▼	Not Free	18	▲	17	▼	28	▼
Pakistan	69	69		Not Free	20		20		29	
Philippines	27	27		Free	10		5		12	
Singapore	40	41	▼	Partly Free	6		14		21	▼
South Korea	33	34	▼	Partly Free	3		14		17	▼
Sri Lanka	58	47	▲	Partly Free	14	▲	13	▲	20	▲
Thailand	62	63	▼	Not Free	9	▲	22	▼	32	▼
Vietnam	76	76		Not Free	13	▲	29	▼	34	
Eurasia										
Armenia	28	28		Free	6	▲	10	▼	12	
Azerbaijan	55	56	▼	Partly Free	13	▲	19	▼	24	
Belarus	62	64	▼	Not Free	15		21	▼	28	▼
Georgia	26	24	▲	Free	7	▲	6	▲	11	
Kazakhstan	60	61	▼	Not Free	14	▲	23		24	▼
Kyrgyzstan	34	35	▼	Partly Free	11	▲	8	▲	16	▼
Russia	60	62	▼	Not Free	10		23	▼	29	▼
Turkey	55	58	▼	Partly Free	13	▲	20	▼	25	▼
Ukraine	33	37	▼	Partly Free	8		10	▼	19	▼
Uzbekistan	79	78	▲	Not Free	19	▲	28		31	
Latin America										
Argentina	27	27		Free	7		8	▲	12	▼
Brazil	30	29	▲	Free	7		6	▲	16	
Colombia	30	32	▼	Partly Free	8		8		16	▼
Cuba	84	81	▲	Not Free	22	▲	27	▲	32	▲
Ecuador	37	37		Partly Free	8	▲	11		18	▼
Mexico	39	39		Partly Free	9	▲	10		20	▼
Venezuela	56	57	▼	Partly Free	17		18		22	▼

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

▼ = Decline ▲ = Improvement Blank = No Change

	Overall				Category Trajectories					
Country	FOTN 2014	FOTN 2015	Overall Trajectory	FOTN 2015 Status	A. Obstacles to Access		B. Limits on Content		C. Vio lations of User Rights	
Middle East & North Africa										
Bahrain	74	72	▲	Not Free	11	▲	27		34	▲
Egypt	60	61	▼	Not Free	14	▲	13	▼	34	▼
Iran	89	87	▲	Not Free	20	▲	31		36	
Jordan	48	50	▼	Partly Free	12		16	▼	22	▼
Lebanon	47	45	▲	Partly Free	13	▲	12		20	▲
Libya	48	54	▼	Partly Free	20	▼	12	▼	22	▼
Morocco	44	43	▲	Partly Free	11		9	▲	23	
Saudi Arabia	73	73		Not Free	15		24		34	
Syria	88	87	▲	Not Free	24	▲	26		37	
Tunisia	39	38	▲	Partly Free	10	▲	8		20	
United Arab Emirates	67	68	▼	Not Free	14		22		32	▼
Sub-Saharan Africa										
Angola	38	39	▼	Partly Free	14	▲	8	▼	17	▼
Ethiopia	80	82	▼	Not Free	23		28		31	▼
Kenya	28	29	▼	Free	9		7		13	▼
Malawi	42	40	▲	Partly Free	15	▲	12	▼	13	▲
Nigeria	33	33		Partly Free	10		8		15	
Rwanda	50	50		Partly Free	11	▲	20	▼	19	
South Africa	26	27	▼	Free	8	▼	8		11	
Sudan	65	65		Not Free	18		19		28	
The Gambia	65	65		Not Free	18	▲	21		26	▼
Uganda	34	36	▼	Partly Free	11		7		18	▼
Zambia	43	40	▲	Partly Free	11	▲	12	▲	17	▲
Zimbabwe	55	56	▼	Partly Free	15		16	▼	25	
Australia, Canada, European Union, Iceland & United States										
Australia	17	19	▼	Free	2		5		12	▼
Canada	15	16	▼	Free	3		4	▼	9	
Estonia	8	7	▲	Free	1		3		3	▲
France	20	24	▼	Free	3		6	▼	15	▼
Germany	17	18	▼	Free	4		5	▼	9	
Hungary	24	24		Free	4	▲	9	▼	11	
Iceland	6	6		Free	1		1		4	
Italy	22	23	▼	Free	4		6		13	▼
United Kingdom	24	24		Free	2		6		16	
United States	19	19		Free	3	▲	2		14	▼

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

▼ = Decline ▲ = Improvement Blank = No Change

Methodology

Freedom on the Net provides analytical reports and numerical scores for 65 countries worldwide. Assigning scores allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. The country reports provide narrative detail to support the scores. *Freedom on the Net* also documents censorship methods used by different countries in an annual chart (see "Key Internet Controls By Country").

The countries were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom. The ratings and reports included in this study particularly focus on developments that took place between June 1, 2014 and May 31, 2015.

Freedom on the Net is a collaborative effort between a small team of Freedom House staff and an extensive network of local researchers and advisors in 65 countries. Our in-country researchers have diverse backgrounds—academia, blogging, traditional journalism, and tech—and track developments from their country of expertise. In the most repressive environments, Freedom House takes care to ensure researchers' anonymity or, in exceptional cases, works with individuals living outside their home country.

What We Measure

The *Freedom on the Net* index measures each country's level of internet and digital media freedom based on a set of methodology questions developed in consultation with international experts to capture the vast array of relevant issues that enable internet freedom (see "Checklist of Questions"). Given increasing technological convergence, the index also measures access and openness of other digital means of transmitting information, particularly mobile phones and text messaging services.

Freedom House does not maintain a culture-bound view of freedom. The project methodology is grounded in basic standards of free expression, derived in large measure from Article 19 of the Universal Declaration of Human Rights:

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers."

This standard applies to all countries and territories, irrespective of geographical location, ethnic or religious composition, or level of economic development.

The project particularly focuses on the transmission and exchange of news and other politically relevant communications, as well as the protection of users' rights to privacy and freedom from both legal and extralegal repercussions arising from their online activities. At the same time, the index acknowledges that in some instances freedom of expression and access to information may be legitimately restricted. The standard for such restrictions applied in this index is that they be implemented only in narrowly defined circumstances and in line with international human rights standards, the rule of law, and the principles of necessity and proportionality. As much as possible, censorship and surveillance policies and procedures should be transparent and include avenues for appeal available to those affected.

The index does not rate governments or government performance per se, but rather the real-world rights and freedoms enjoyed by individuals within each country. While digital media freedom may be primarily affected by state actions, pressures and attacks by nonstate actors, including the criminal underworld, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental, including private corporations.

The Scoring Process

The methodology includes 21 questions and nearly 100 subquestions, divided into three categories:

- **Obstacles to Access** details infrastructural and economic barriers to access, legal and ownership control over internet service providers , and independence of regulatory bodies;
- **Limits on Content** analyzes legal regulations on content, technical filtering and blocking of websites, self-censorship, the vibrancy and diversity of online news media, and the use of digital tools for civic mobilization;

- **Violations of User Rights** tackles surveillance, privacy, and repercussions for online speech and activities, such as imprisonment, extralegal harassment, or cyberattacks.

Each question is scored on a varying range of points. The subquestions guide researchers regarding factors they should consider while evaluating and assigning points, though not all apply to every country. Under each question, a lower number of points is allotted for a more free situation, while a higher number of points is allotted for a less free environment. Points add up to produce a score for each of the subcategories, and a country's total points for all three represent its final score (0-100). Based on the score, Freedom House assigns the following internet freedom ratings:

- Scores 0-30 = Free
- Scores 31-60 = Partly Free
- Scores 61-100 = Not Free

After researchers submitted their draft scores in 2015, Freedom House convened five regional review meetings and numerous international conference calls, attended by Freedom House staff and over 70 local experts, scholars, and civil society representatives from the countries under study. During the meetings, participants reviewed, critiqued, and adjusted the draft scores—based on set coding guidelines—through careful consideration of events, laws, and practices relevant to each item. After completing the regional and country consultations, Freedom House staff did a final review of all scores to ensure their comparative reliability and integrity.

Key Internet Controls Explained

In the Key Internet Controls table (page 16-17), Freedom House staff document the prevalence of different censorship methods by marking incidents of their occurrence in each country. Incidents are based on *Freedom on the Net* research and verified by in-country researchers. Inclusion in the table indicates the internet control occurred at least once during the coverage period of the report, unless otherwise indicated.

1. **Social media or communications apps blocked:** Entire platforms temporarily or permanently blocked to prevent communication and information sharing.
2. **Political, social, or religious content blocked:** Blocking or filtering of domains, URLs, or keywords, to limit access to specific content.
3. **Localized or nationwide ICT shut down:** Intentional disruption of internet or cellphone networks in response to political or social events, whether temporary or long term.
4. **Progovernment commentators manipulate online discussions:** Strong indications that individuals are paid to distort the digital information landscape in the government's favor, without acknowledging sponsorship.
5. **New law or directive increasing censorship or punishment passed:** Any legislation adopted or amended during the coverage period, or any directive issued, to censor or punish legitimate online activity.
6. **New law or directive increasing surveillance or restricting anonymity passed:** Any legislation adopted or amended during the coverage period, or any directive issued, to surveil or expose the identity of citizens using the internet with legitimate intent.
7. **Blogger or ICT user arrested, imprisoned, or in prolonged detention for political or social content:** Any arrest or detention that is credibly perceived to be in reprisal for digital expression, including trumped up charges. Brief detentions for interrogation are not reflected.
8. **Blogger or ICT user physically attacked or killed (including in custody):** Any physical attack that is credibly perceived to be in reprisal for digital expression, including kidnapping and torture.
9. **Technical attacks against government critics and human rights organizations:** Cyberattacks against individuals sharing information perceived as critical, with the clear intent of disabling content or exposing user data, and motives that align with those of agencies that censor and surveil the internet. Targets may include critics in exile, but not transnational cyberattacks, even with political motives.

Checklist of Questions

- Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- A combined score of 0-30=Free, 31-60=Partly Free, 61-100=Not Free.

A. OBSTACLES TO ACCESS (0-25 POINTS)

1. To what extent do infrastructural limitations restrict access to the internet and other ICTs? (0-6 points)

- Does poor infrastructure (electricity, telecommunications, etc.) limit citizens' ability to receive internet in their homes and businesses?
- To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?
- To what extent is there internet and mobile phone access, including data connections or satellite?
- Is there a significant difference between internet and mobile phone penetration and access in rural versus urban areas or across other geographical divisions?
- To what extent are broadband services widely available in addition to dial-up?

2. Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)

- In countries where the state sets the price of internet access, is it prohibitively high?
- Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?
- Do low literacy rates (linguistic and "digital literacy") limit citizens' ability to use the internet?
- Is there a significant difference between internet penetration and access across ethnic or socioeconomic societal divisions?
- To what extent are online software, news, and other information available in the main local languages spoken in the country?

3. Does the government impose restrictions on ICT connectivity and access to particular social media and communication apps permanently or during specific events? (0-6 points)

- Does the government place limits on the amount of bandwidth that access providers can supply?
- Does the government use control over internet infrastructure (routers, switches, etc.) to limit connectivity, permanently or during specific events?
- Does the government centralize telecommunications infrastructure in a manner that could facilitate control of content and surveillance?
- Does the government block protocols and tools that allow for instant, person-to-person communication (VOIP, instant messaging, text messaging, etc.), particularly those based outside the country (e.g. Skype, WhatsApp, etc)?
- Does the government block protocols, social media, and/or communication apps that allow for information sharing or building online communities (video-sharing, social-networking sites, comment features, blogging platforms, etc.) permanently or during specific events?
- Is there blocking of certain tools that enable circumvention of online filters and censors?

4. Are there legal, regulatory, or economic obstacles that prevent the existence of diverse business entities providing access to digital technologies? (0-6 points)

Note: Each of the following access providers are scored separately:

1a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)

1b. Cybercafes and other businesses entities that allow public internet access (0-2 points)

1c. Mobile phone companies (0-2 points)

- Is there a legal or de facto monopoly over access providers or do users have a choice of access provider, including ones privately owned?
- Is it legally possible to establish a private access provider or does the state place extensive legal or regulatory controls over the establishment of providers?
- Are registration requirements (i.e. bureaucratic "red tape") for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?
- Does the state place prohibitively high fees on the establishment and operation of access providers?

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

- Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?
- Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' interests?
- Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?
- Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?
- Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?

B. LIMITS ON CONTENT (0-35 POINTS)

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

- Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?
- Is there significant filtering of text messages or other content transmitted via mobile phones?
- Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of email or text messages, etc?
- Are methods such as deep-packet inspection used for the purposes of preventing users from accessing certain content or for altering the content of communications en route to the recipient, particularly with regards to political and social topics?

2. To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? (0-4 points)

- To what extent are non-technical measures—judicial or extra-legal—used to order the deletion of content from the internet, either prior to or after its publication?
- To what degree do government officials or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?
- Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?
- Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?

3. To what extent are restrictions on internet and ICT content transparent, proportional to the stated aims, and accompanied by an independent appeals process? (0-4 points)

- Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?
- Are state authorities transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?
- Do state authorities block more types of content than they publicly declare?
- Do independent avenues of appeal exist for those who find content they produced to have been subjected to censorship?

4. Do online journalists, commentators, and ordinary users practice self-censorship? (0-4 points)

- Is there widespread self-censorship by online journalists, commentators, and ordinary users in state-run online media, privately run websites, or social media applications?
- Are there unspoken "rules" that prevent an online journalist or user from expressing certain opinions in ICT communication?
- Is there avoidance of subjects that can clearly lead to harm to the author or result in almost certain censorship?

5. To what extent is the content of online sources of information determined or manipulated by the government or a particular partisan interest? (0-4 points)

- To what degree do government officials or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?
- Do authorities issue official guidelines or direc-

tives on coverage to online media outlets, blogs, etc., including instructions to marginalize or amplify certain comments or topics for discussion?
- Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?
- Does the government employ, or encourage content providers to employ, individuals to post pro-government remarks in online bulletin boards and chat rooms?
- Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?

6. Are there economic constraints that negatively impact users' ability to publish content online or online media outlets' ability to remain financially sustainable? (0-3 points)
- Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, email applications, blog hosting platforms, etc.) to be economically viable?
- Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?
- Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?
- To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect "net neutrality" with regard to content)?
- To what extent do users have access to free or low-cost blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?

7. To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content? (0-4 points)
- Are people able to access a range of local and international news sources via the internet or text messages, despite efforts to restrict the flow of information?
- Does the public have ready access to media outlets or websites that express independent, balanced views?
- Does the public have ready access to sources of information that represent a range of political and social viewpoints?
- To what extent do online media outlets and blogs represent diverse interests within society, for example through websites run by community organizations or religious, ethnic and other minorities?
- To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?

8. To what extent have individuals successfully used the internet and other ICTs as sources of information and tools for mobilization, particularly regarding political and social issues? To what extent are such mobilization tools available without government restriction? (0-6 points)
- To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or the behavior of other powerful societal actors?
- To what extent are online communication tools or social networking sites (e.g. Twitter, Facebook) used as a means to organize politically, including for "real-life" activities?
- Are mobile phones and other ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?

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

1. To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)
- Does the constitution contain language that provides for freedom of speech and of the press generally?
- Are there laws or legal decisions that specifically protect online modes of expression?
- Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?
- Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?
- Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?

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

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

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

- Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?
- Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via email or text messages?
- Does the lack of an independent judiciary or other limitations on adherence to the rule of law hinder fair proceedings in ICT-related cases?
- Are individuals subject to abduction or arbitrary detention as a result of online activities, including membership in certain online communities?
- Are penalties for "irresponsible journalism" or "rumor mongering" applied widely?
- Are online journalists, bloggers, or others regularly prosecuted, jailed, or fined for libel or defamation (including in cases of "libel tourism")?

4. Does the government place restrictions on anonymous communication or require user registration? (0-4 points)

- Are website owners, bloggers, or users in general required to register with the government?
- Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names or register with the government?
- Are users prohibited from using encryption software to protect their communications?
- Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?

5. To what extent is there state surveillance of internet and ICT activities without judicial or other independent oversight, including systematic retention of user traffic data? (0-6 points)

- Do the authorities regularly monitor websites, blogs, and chat rooms, or the content of email and mobile text messages?
- To what extent are restrictions on the privacy of digital media users transparent, proportional to the stated aims, and accompanied by an independent process for lodging complaints of violations?
- Where the judiciary is independent, are there procedures in place for judicial oversight of surveillance and to what extent are these followed?
- Where the judiciary lacks independence, is there another independent oversight body in place to guard against abusive use of surveillance technology and to what extent is it able to carry out its responsibilities free of government interference?
- Is content intercepted during internet surveillance admissible in court or has it been used to convict users in cases involving free speech?

6. To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users? (0-6 points)

Note: Each of the following access providers are scored separately:

6a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)

6b. Cybercafes and other business entities that allow public internet access (0-2 points)

6c. Mobile phone companies (0-2 points)

- Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?
- Are access providers prosecuted for not doing so?
- Does the state attempt to control access provid-

ers through less formal methods, such as codes of conduct?
- Can the government obtain information about users without a legal process?

7. Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor? (0–5 points)
- Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?
- Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?
- Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?
- Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?

8. Are websites, governmental and private entities, ICT users, or service providers subject to widespread "technical violence," including cyberattacks, hacking, and other malicious threats? (0-3 points)
- Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks (e.g. cyberespionage, data gathering, DDoS attacks), including those originating from outside of the country?
- Have websites belonging to opposition or civil society groups within the country's boundaries been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?
- Are websites or blogs subject to targeted technical attacks as retribution for posting certain content (e.g. on political and social topics)?
- Are laws and policies in place to prevent and protect against cyberattacks (including the launching of systematic attacks by nonstate actors from within the country's borders) and are they enforced?

Contributors

Freedom House Research Team

- Sanja Kelly, Project Director, *Freedom on the Net*
- Mai Truong, Senior Program Officer (Africa)
- Madeline Earp, Research Analyst (Asia)
- Laura Reed, Research Analyst (Eurasia, EU & Western countries)
- Adrian Shahbaz, Research Analyst (MENA & EU)
- Alexandra Ellerbeck, Senior Research Assistant (Latin America)

Report Authors and Advisors

- **Argentina:** Eduardo Andres Bertoni, Director, Center for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law, Argentina; Daniela Schnidrig, Researcher, CELE
- **Armenia:** Seda Muradyan, Armenia Country Director, Institute for War and Peace Reporting; Samvel Martirosyan, Head of Board, Institute for Strategic and Innovative Research
- **Australia:** Dr. Alana Maurushat, Senior Lecturer, Faculty of Law, and Co-Director, Cyberspace Law and Policy Community, The University of New South Wales
- **Azerbaijan:** Arzu Geybulla, Azerbaijani journalist and blogger
- **Bangladesh:** Dr. Faheem Hussain, Assistant Professor, Department of Technology and Society, State University of New York (SUNY) Korea
- **Brazil:** Fabrício Bertini Pasquot Polido, Professor, Law School of the Federal University of Minas Gerais, and Head of the Center for International Studies on Internet, Innovation, and Intellectual Property (GNET); Carolina Rossini, Vice President of International Policy, Public Knowledge, and Board Member, Open Knowledge Foundation, InternetLab, and CodingRights
- **Cambodia:** Sopheap Chak, Executive Director, Cambodian Center for Human Rights, and human rights blogger
- **Canada:** Michael Geist, Canada Research Chair in Internet and E-commerce Law, Faculty of Law, University of Ottawa
- **China:** Sarah Hoffman, Youth Free Expression Program Manager, National Coalition Against Censorship, and China researcher; Wen Yunchao ("Beifeng"), Chinese blogger and activist
- **Colombia:** Law, Internet, and Society Group, Fundación Karisma
- **Cuba:** Ernesto Hernández Busto, Cuban journalist and writer
- **Estonia:** Linnar Viik, Associate Professor, Estonian IT College
- **France:** Jean-Loup Richet, Researcher, University of Nantes
- **Georgia:** Teona Turashvili, Analyst, Institute for Development of Freedom of Information (IDFI)
- **Germany:** Philipp Otto, Founder and Head, iRights. Lab think tank and iRights.Media publishing house, Editor in Chief, iRights.info, political strategist, advisor to the German government and companies; Henning Lahmann, Policy Analyst, iRights.Lab
- **Hungary:** Borbála Tóth, independent researcher based in Budapest
- **Iceland:** Caroline Nellemann, independent consultant, specialist in digital media and civic engagement
- **India:** Chinmayi Arun, Research Director, Center for Communication Governance at National Law University, Delhi; Sarvjeet Singh, Senior Fellow and Project Manager, Centre for Communication Governance; Parul Sharma, Student, B.A., LL.B. (Hons.), National Law University; with research assistance from students Nishtha Sinha and Vaibhav Dutt, B.A., LL.B. (Hons.), National Law University
- **Indonesia:** Enda Nasution, Co-Founder, Sebangsa.com, and independent blogger
- **Iran:** Mahmood Enayat, Director, Small Media
- **Italy:** Giampiero Giacomello, Associate Professor of International Relations, University of Bologna
- **Japan:** Dr. Leslie M. Tkach-Kawasaki, Associate Professor, University of Tsukuba
- **Jordan:** Lina Ejeilat, Co-founder and Executive Editor, 7iber
- **Kazakhstan:** Adilzhan Nurmakov, Senior Lecturer, KIMEP University
- **Kenya:** Grace Githaiga, Associate, Kenya ICT Action Network (KICTANet)
- **Kyrgyzstan:** Artem Goryainov, IT Programs Director, Public Foundation CIIP

- **Lebanon:** Firas Talhouk, Researcher, Samir Kassir Foundation
- **Libya:** Maraim Masoud Elbadri, Business Developer, Tatweer Research
- **Malawi:** Gregory Gondwe, Bureau Chief, Times Media Group, Malawi
- **Malaysia:** K. Kabilan, Managing Editor, BeritaDaily.com, and online media consultant
- **Mexico:** Jorge Luis Sierra, Knight International Journalism Fellow, International Center for Journalists, and award-winning Mexican journalist
- **Morocco:** Bouziane Zaid, Assistant Professor of Media and Communication, Al Akhawayn University in Ifrane
- **Myanmar:** Min Zin, Burmese journalist, and Contributor, Foreign Policy Democracy Lab
- **Nigeria:** 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria
- **Pakistan:** Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan; Muhammad Ismael Khan, Research Associate, Digital Rights Foundation
- **Philippines:** Jacques D.M. Gimeno, independent researcher based in Manila
- **Singapore:** Cherian George, Associate Professor, School of Communication, Hong Kong Baptist University
- **South Africa:** Alex Comninos, independent researcher
- **South Korea:** Dr. Yenn Lee, Doctoral Training Advisor, School of Oriental and African Studies, University of London
- **Sri Lanka:** N. V. Nugawela, independent writer and researcher
- **Sudan:** Azaz Elshami, independent researcher and development consultant
- **Syria:** Dlshad Othman, Information Security Manager, Information Safety & Capacity Project (ISC)
- **Uganda:** Lillian Nalwoga, Policy Officer, CIPESA, and President, Internet Society Uganda Chapter
- **Ukraine:** Tetyana Lokot, Ukrainian journalist; Contributing Editor, RuNet Echo, Global Voices; and Doctoral Candidate, Philip Merrill College of Journalism, University of Maryland
- **United Kingdom:** LSE Media Policy Project, London School of Economics and Political Science
- **United States:** Open Technology Institute, New America
- **Uzbekistan:** Dr. Zhanna Hördegen, Research Associate, University Research Priority Program (URPP) Asia and Europe, University of Zurich, and independent consultant
- **Venezuela:** Raisa Urribarri, Director, Communications Lab for Teaching, Research and Community Extension (LIESR) at the University of Los Andes
- **Zambia:** Brenda Bukowa, Lecturer and Researcher, Department of Mass Communication, University of Zambia

The analysts for the reports on Angola, Bahrain, Belarus, Ecuador, Egypt, Ethiopia, The Gambia, Russia, Rwanda, Saudi Arabia, Thailand, Tunisia, Turkey, United Arab Emirates, Vietnam and Zimbabwe are independent internet researchers who have requested to remain anonymous. *Freedom on the Net* intern Liridona Malota provided invaluable research and administrative assistance in the production of the 2015 edition of the report.

“Digital activism has been and remains a vital driver of change around the world, particularly in societies that lack political rights and press freedom.”

Freedom House

Freedom House is a nonprofit, nonpartisan organization that supports democratic change, monitors freedom, and advocates for democracy and human rights.

1850 M Street NW, 11th Floor
Washington, DC 20036

120 Wall Street, 26th Floor
New York, NY 10005

www.freedomhouse.org
facebook.com/FreedomHouseDC
@FreedomHouseDC

202.296.5101 | info@freedomhouse.org