Tightening the Net:
Governments Expand Online Controls

Freedom House

FREEDOM ON THE NET 2014

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

This booklet is a summary of findings for the 2014 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.

Cover: Photo from an antigovernment protest outside the ruling party's headquarters in Bangkok, Thailand on November 29, 2013. *Photo: Shutterstock.*

FREEDOM
ON THE NET
2014

Tightening the Net: Governments Expand Online Controls

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

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

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

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

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

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

Key Reasons for Decline in Internet Freedom, 2013–14:

- Proliferation of repressive laws
- Increased surveillance
- New regulatory controls over online media
- More arrests of social-media users
- Intensified demands on private sector
- New threats facing women and LGBTI population
- More sophisticated and widespread cyberattacks

Blocking and filtering—once the most widespread methods of censorship—are still very common, but many countries now prefer to simply imprison users who post undesirable content, thereby deterring others and encouraging self-censorship. This approach can present the appearance of a technically uncensored internet while effectively limiting certain types of speech. Meanwhile, physical violence against internet users appears to have decreased in scope. In 2013, Freedom House documented 26 countries where government critics and human rights defenders were subjected to beatings and other types of physical violence in connection with their online activity; that number fell to 22 in 2014.

Tracking the Global Decline

To illuminate the nature of the principal threats in this rapidly changing environment, Freedom House conducted a comprehensive study of internet freedom in 65 countries around the world. This report is the fifth in its series and focuses on developments that occurred between May 2013 and May 2014. The previous edition, covering 60 countries, was published in October 2013. *Freedom on the Net 2014* assesses a greater variety of political systems than its predecessors, while tracing improvements and declines in the countries examined in previous editions. Over 70 researchers, nearly all based in the countries they analyzed, contributed to the project by examining laws and practices relevant to the internet, testing the accessibility of select websites, and interviewing a wide range of sources.

Of the 65 countries assessed, 36 have experienced a negative trajectory since May 2013.

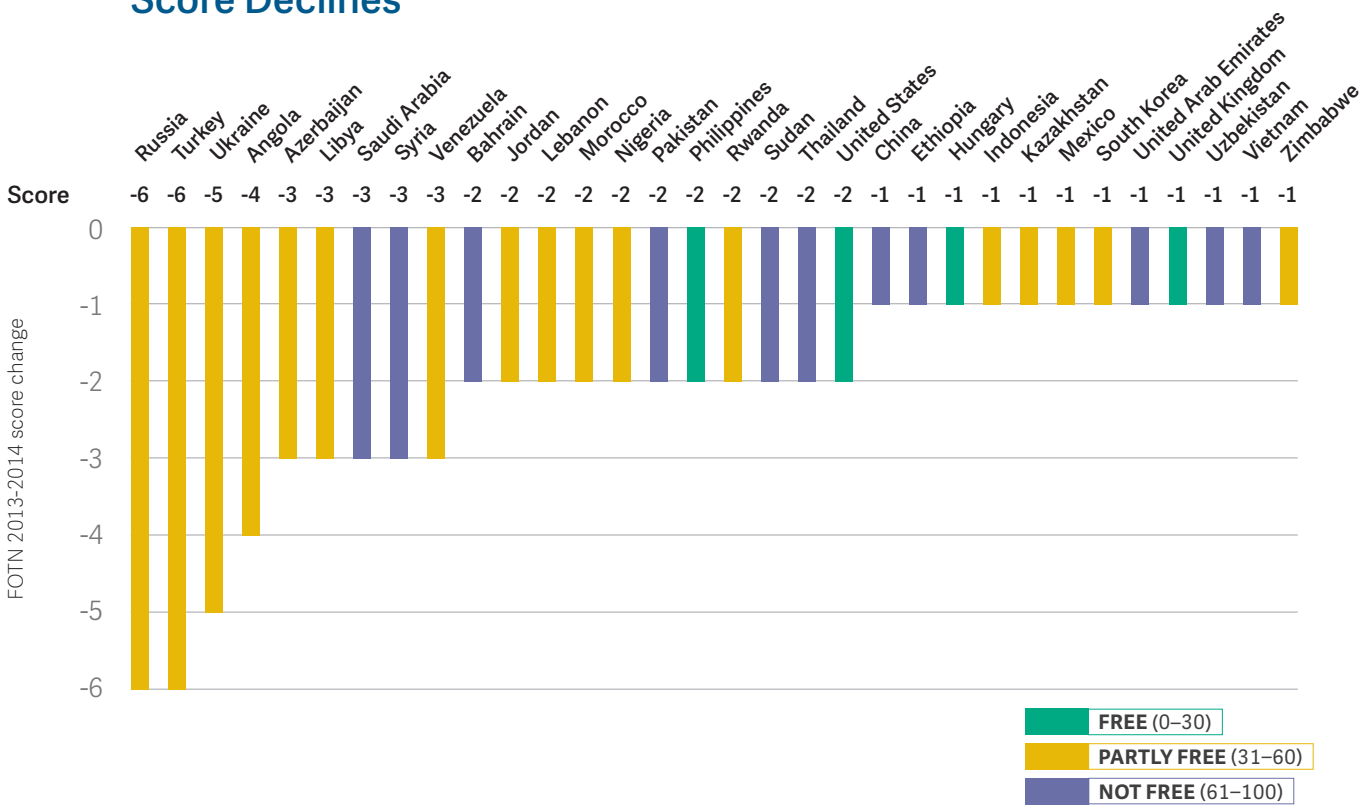
Of the 65 countries assessed, 36 have experienced a negative trajectory since May 2013. The most significant declines were in Russia, Turkey, and Ukraine. The Russian government took multiple steps to increase control over the online sphere, particularly in advance of the Sochi Olympic Games and during the ongoing crisis in Ukraine. In Turkey, the blocking of social media, limits on circumvention tools, cyberattacks against opposition news sites, and assaults on online journalists were among the most prominent threats during the year. Ukraine's standing declined primarily due to violence targeting social-media users and online journalists during the Euromaidan protests, an increase in cyberattacks, and new evidence revealing the extent to which the administration of ousted president Viktor Yanukovych had been conducting online surveillance of activists, journalists, and opposition leaders.

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

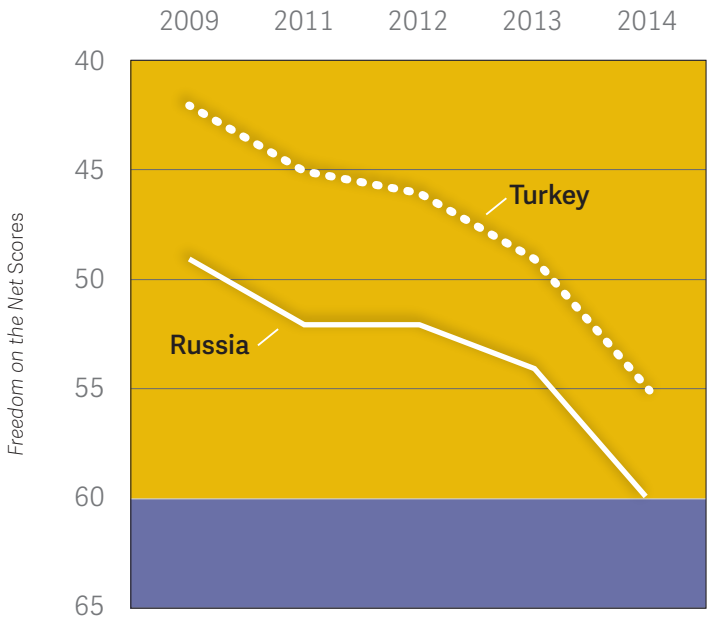
Very few countries registered any gains in internet freedom, and the improvements that were recorded largely reflected less vigorous application of existing internet controls compared with the previous year, rather than genuinely new and positive steps taken by the government. The year's biggest improvement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

Another country that registered a notable improvement is Brazil, where after years of debate and revision, lawmakers approved a bill known as the Marco Civil da Internet that contains important provisions governing net neutrality and ensuring strong privacy protections. Freedom House also documented an improvement in Belarus, mainly because the political environment was less volatile and the government eased enforcement of some restrictions, even as citizens increasingly used the internet to voice their views.

Score Declines



Five-Year Declines in Russia and Turkey



Russia's score declined by 11 points over the past 5 years. Since Putin's return to the presidency in 2012, the government has enacted multiple laws to block online content, including critical or opposition media outlets. Individuals are subject to prosecution and physical violence for their internet activity and increasingly extensive surveillance of ICTs lacks sufficient judicial oversight.

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

FREE (0–30)
PARTLY FREE (31–60)
NOT FREE (61–100)

Major Trends

New Legal Measures Curb Internet Freedom

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In Turkey, after audio recordings implicating high-level officials in a corruption scandal were leaked on YouTube and SoundCloud, new legal measures

empowered the state regulator to block websites without a court order in cases that violate privacy or are considered "discriminatory or insulting." The regulator later blocked YouTube to suppress an unverified recording of a national security meeting. Twitter was also blocked after refusing to suspend user accounts. President Recep Tayyip Erdoğan, who was prime minister at the time, has vowed to "wipe out Twitter" and called social media the "worst menace to society."

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

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

Of the 65 countries studied in Freedom on the Net 2014, 19 passed new legislation that increased surveillance or restricted user anonymity.

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

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

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

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

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

Arrests and Reprisals Increase for Social-Media Users

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

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

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

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

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

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

Internet users were tried not only for what they posted online, but also for content found on their electronic devices. In Thailand, a man was sentenced to seven years in prison after police confiscated his computer and discovered pictures that were deemed insulting to the king. He was convicted of "attempting" to commit lèse-majesté—a charge with no legal basis—as investigators argued that he intended to upload the material to the internet eventually.

Online Journalists and Bloggers Face Greater Pressure

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

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

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

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

Online journalists and others who publish independent reporting online were arrested in at least 25 countries during the coverage period. In Ethiopia, six writers from the *Zone9* news blog were arrested in April 2014 and face charges related to accepting foreign funding and inciting violence through social media. In Iran, 16 employees of the gadget review site Narenji were arrested over alleged links to foreign governments and "anti-Iranian media," with some apparently charged due to their participation in training programs run by the Persian service of the British Broadcasting Corporation (BBC), which the Iranian government linked to the British intelligence agency MI6. Eleven of the defendants were later found guilty, and the website's founder received the heaviest sentence—11 years in prison.

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

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

Emerging Threats

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

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

Data Localization

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

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

In July 2013, the Vietnamese government issued Decree 72, which, among other things, requires international internet companies to establish at least one server in the country, subject to local law and oversight. Despite the fact that numerous international organizations criticized the original draft of the decree

as a significant threat to free speech and privacy, the revised drafts maintained the data localization requirement, though it remains unclear how or whether it will be enforced.

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

Harassment of Women and LGBTI Users

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

Internet freedom is particularly tenuous for LGBTI people and women.

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

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

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

Lack of Cybersecurity

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

So-called spear phishing has emerged as one of the most effective techniques for hijacking online accounts and collecting sensitive information. Victims receive customized e-mail messages that typically direct them to an official-looking page, run by the hackers, where they are prompted to enter their e-mail or social-media credentials. These sorts of attacks were employed by the Syrian Electronic Army against international news organizations such as the *New York Times*, *Global Post*, CNN, and *Forbes* over the past year.

Once in control of an opposition website or social-media account, hackers can post hyperlinks to online petitions or exciting news stories to lure users into clicking. These links often have hidden tracking capabilities that can ascertain a user's location. According to a report by BahrainWatch, malicious links have been used to identify and arrest several anonymous Twitter users who were outspoken against the government in that country. The increased use of "social engineering"—essentially tricking users into revealing information—and account hijacking has reinforced the idea that one's own digital security often depends on the actions and judgment of those in one's broader social or professional network.

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

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

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

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

The Global Struggle for Internet Freedom

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

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

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

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

These legislative and judicial successes notably occurred in democratic states, where the rule of law prevails and governments are generally held accountable to citizens and civil society. In Brazil, for

example, the draft of the Marco Civil was the result of a collaborative process that included input from civil society and ordinary citizens, and it had support from members of Congress and the president.

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

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

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

Key Internet Controls by Country

Country (by FOTN 2014 ranking)	FOTN 2014 Status (F=Free, PF=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 for political or social writings	Online journalist/blogger/ICT user physically attacked or killed (including in custody)	Technical attacks against government critics and human rights organizations	TOTAL # of Key Internet Controls employed in 2013-2014, by country
Iceland	F										0
Estonia	F										0
Canada	F										0
Australia	F						X				1
Germany	F										0
United States	F										0
France	F						X				1
Italy	F					X					1
Japan	F										0
Hungary	F					X					1
United Kingdom	F						X				1
Georgia	F										0
South Africa	F						X				1
Argentina	F						X				1
Phillipines	F										0
Armenia	F									X	1
Kenya	F					X					1
Brazil	F					X					1
Colombia	F								X	X	2
Nigeria	PF			X			X	X		X	4
South Korea	PF		X		X			X			3
Ukraine	PF			X	X				X	X	4
Kyrgyzstan	PF	X	X		X	X	X				5
Uganda	PF					X				X	2
Ecuador	PF				X	X				X	3
Angola	PF							X	X	X	3
Mexico	PF				X		X		X	X	4
Tunisia	PF						X	X		X	3
Singapore	PF					X		X			2
India	PF		X	X	X			X			4
Indonesia	PF		X					X			2
Malawi	PF						X	X			2
Malaysia	PF		X		X			X		X	4

Country (by FOTN 2014 ranking)	FOTN 2014 Status (F=Free, PF=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 for political or social writings	Online journalist/blogger/ICT user physically attacked or killed (including in custody)	Technical attacks against government critics and human rights organizations	TOTAL # of Key Internet Controls employed in 2013-2014, by country
Zambia	PF		X					X			2
Morocco	PF		X		X			X		X	4
Cambodia	PF		X								1
Lebanon	PF		X					X	X	X	4
Jordan	PF		X			X		X			3
Libya	PF			X					X		2
Bangladesh	PF		X			X		X	X		4
Rwanda	PF		X		X		X	X		X	5
Azerbaijan	PF	X	X		X	X		X	X	X	7
Turkey	PF	X	X			X	X	X	X	X	7
Zimbabwe	PF		X				X	X		X	4
Venezuela	PF	X	X	X	X		X	X	X	X	8
Sri Lanka	PF		X								1
Egypt	PF			X	X			X	X	X	5
Kazakhstan	PF	X	X		X	X		X		X	6
Myanmar	PF					X	X	X		X	4
Russia	PF		X		X	X	X	X	X	X	7
Belarus	NF		X		X			X		X	4
Thailand	NF	X	X	X		X		X	X		6
Sudan	NF		X	X	X			X		X	5
The Gambia	NF	X	X	X		X		X		X	6
United Arab Emirates	NF	X	X					X	X		4
Pakistan	NF	X	X	X		X		X	X		6
Saudi Arabia	NF	X	X		X	X		X	X	X	7
Bahrain	NF	X	X		X			X	X	X	6
Vietnam	NF		X		X	X	X	X	X	X	7
Uzbekistan	NF	X	X		X		X	X		X	6
Ethiopia	NF	X	X	X	X		X	X		X	7
Cuba	NF	X	X		X			X	X		5
China	NF	X	X	X	X	X		X	X	X	8
Syria	NF	X	X	X				X	X	X	6
Iran	NF	X	X		X			X	X	X	6
TOTAL		17	34	13	24	21	19	38	22	32	

X = Internet control observed during the May 2013–May 2014 coverage period

X = Internet control observed after May 31, 2014 until the time of writing

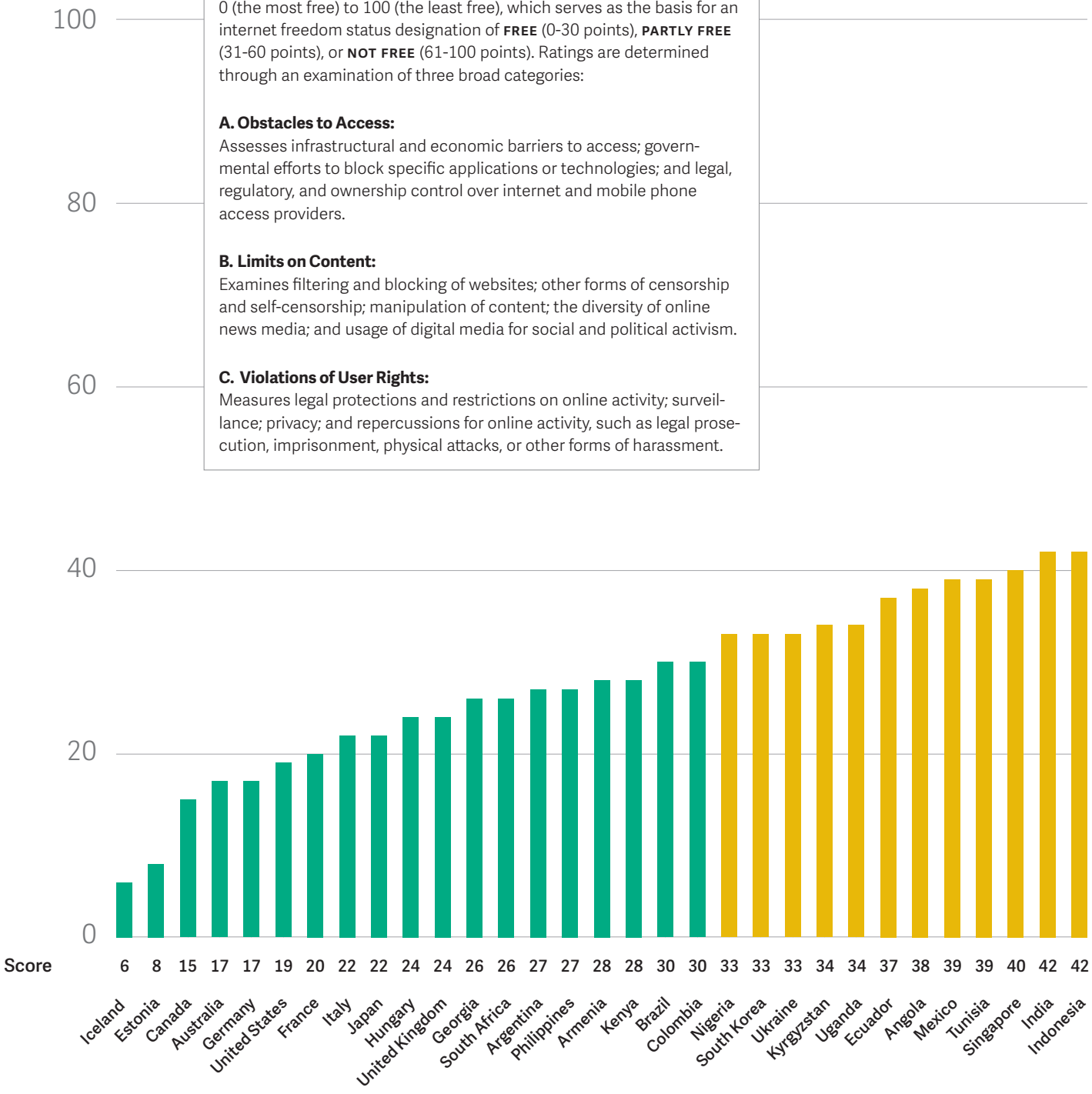
65 Country Score Comparison

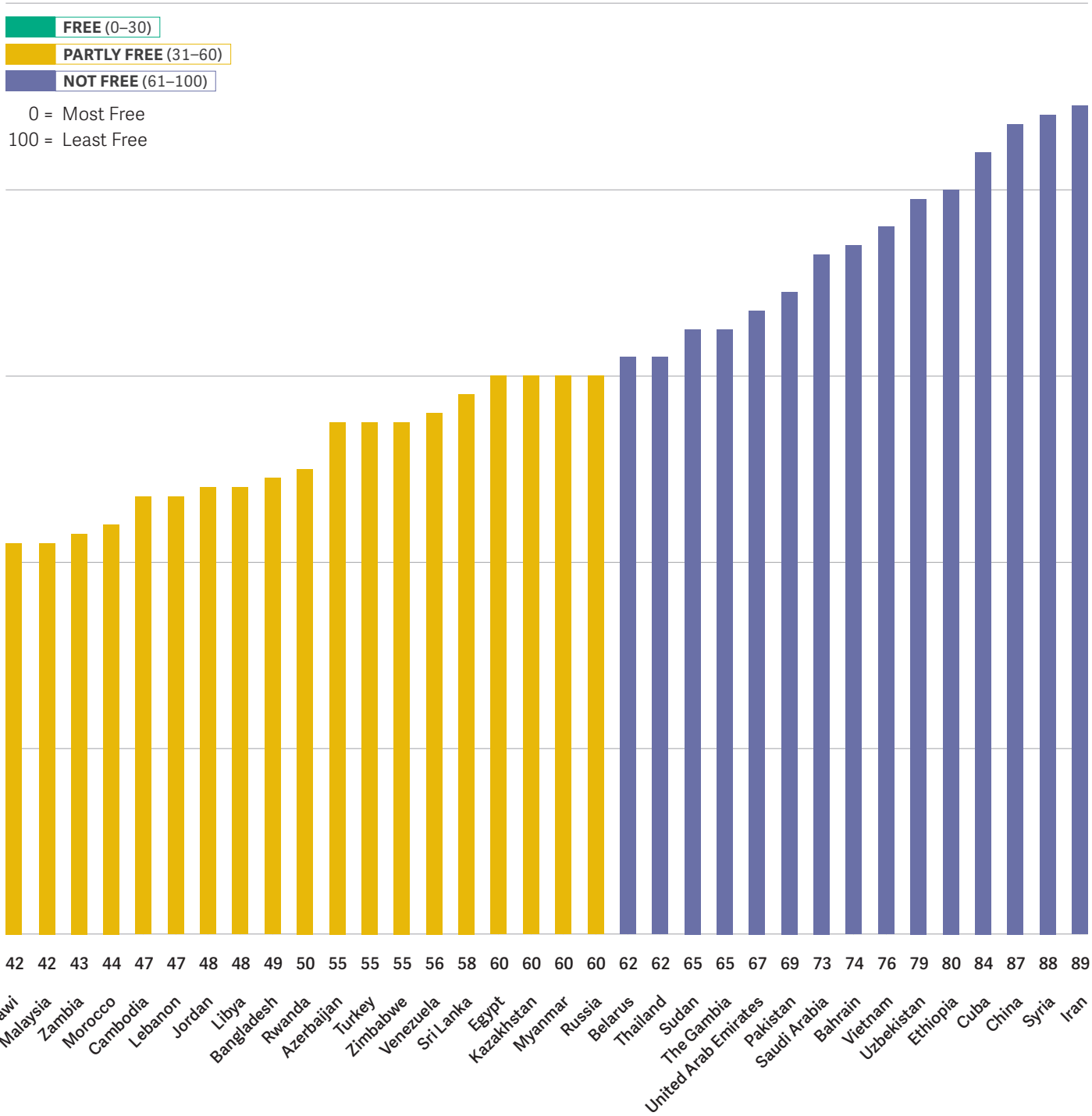
Freedom on the Net measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of **FREE** (0-30 points), **PARTLY FREE** (31-60 points),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

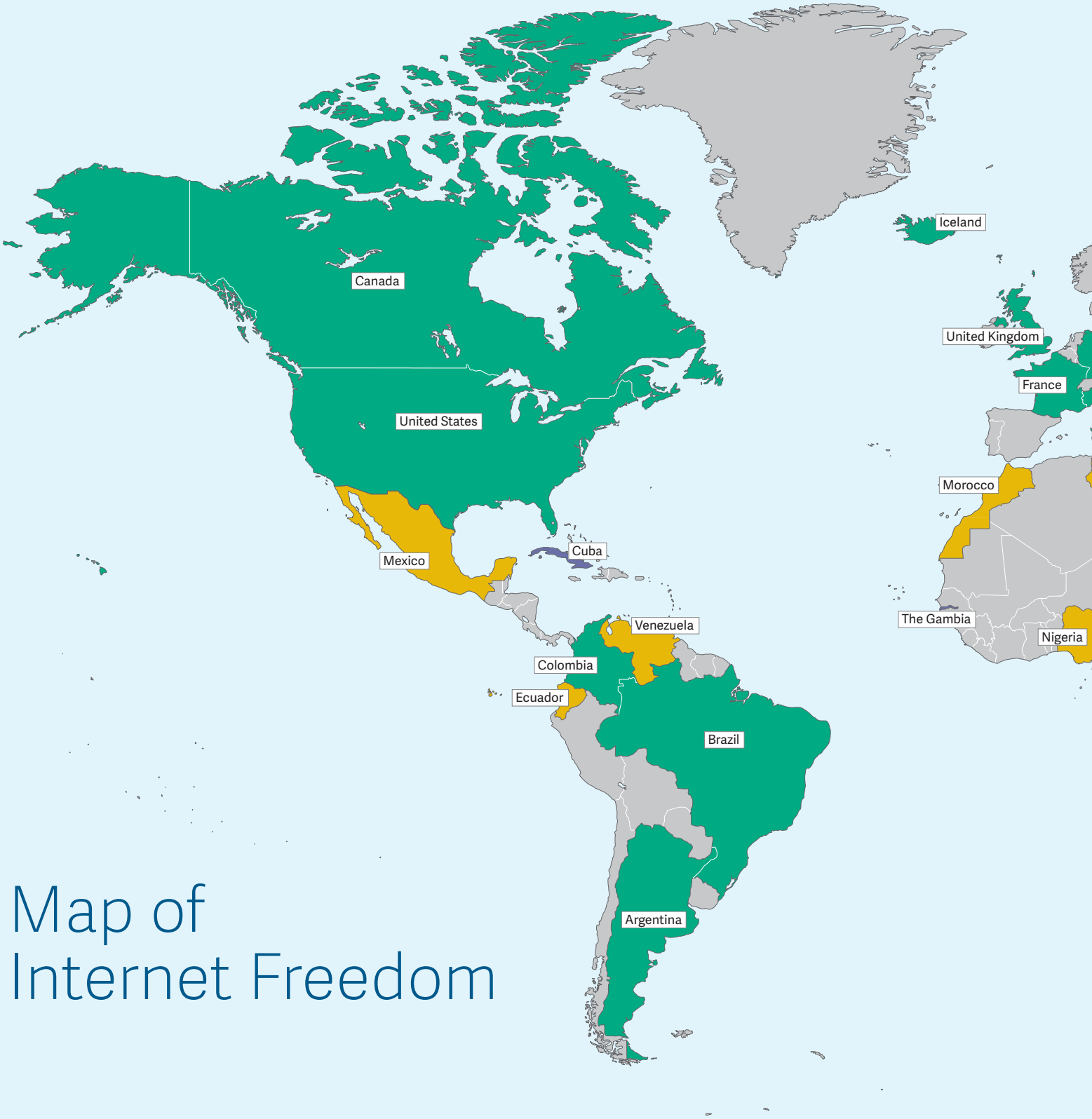
A. Obstacles to Access:
Assesses infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; and legal, regulatory, and ownership control over internet and mobile phone access providers.

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.

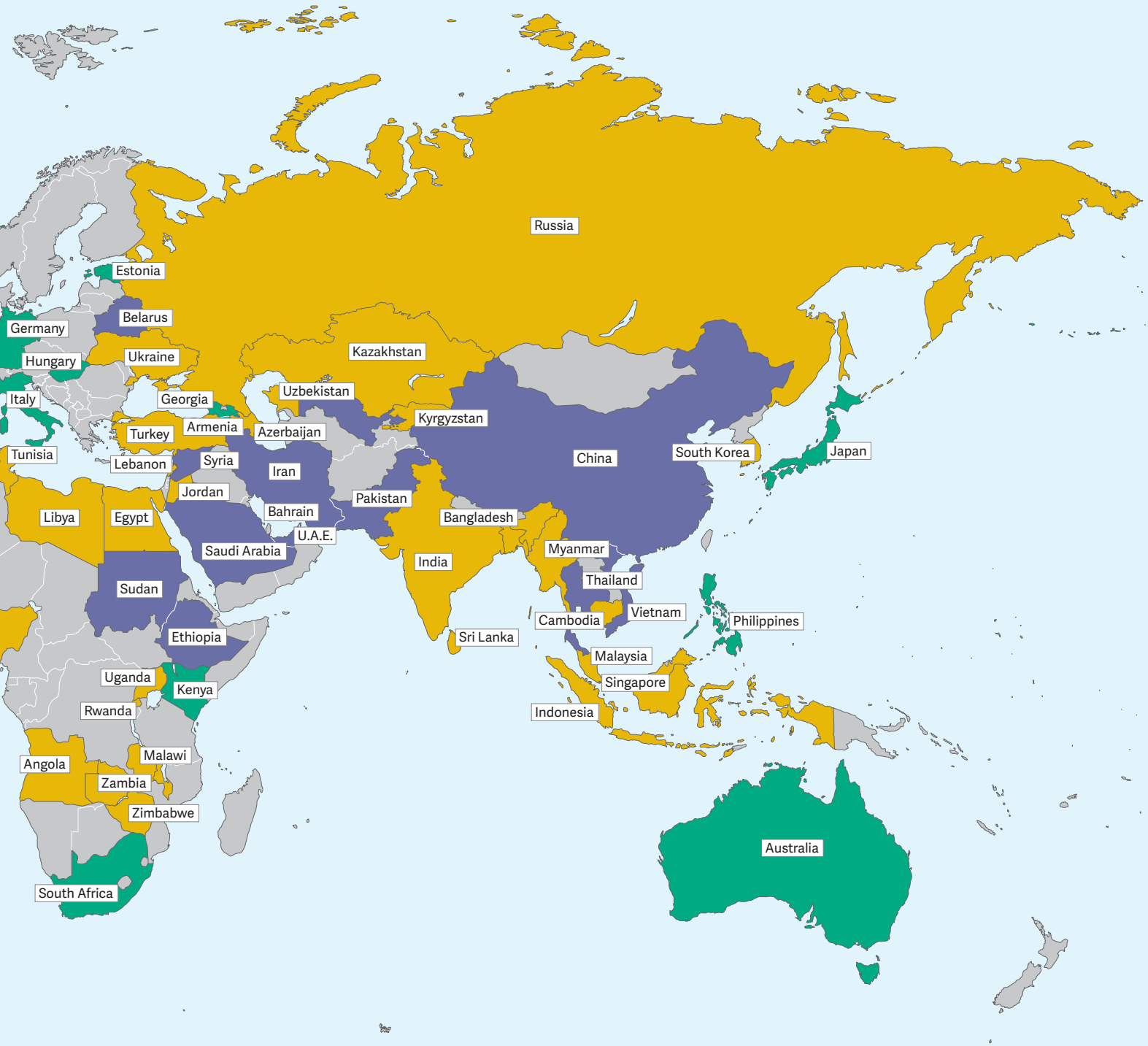



FREE (0–30)
PARTLY FREE (31–60)
NOT FREE (61–100)
0 = Most Free
100 = Least Free
42 42 43 44 47 47 48 48 49 50 55 55 55 56 58 60 60 60 60 62 62 65 65 67 69 73 74 76 79 80 84 87 88 89
Malawi
Malaysia
Zambia
Morocco
Cambodia
Lebanon
Jordan
Libya
Bangladesh
Rwanda
Azerbaijan
Turkey
Zimbabwe
Venezuela
Sri Lanka
Egypt
Kazakhstan
Myanmar
Russia
Belarus
Thailand
Sudan
The Gambia
United Arab Emirates
Pakistan
Saudi Arabia
Bahrain
Vietnam
Uzbekistan
Ethiopia
Cuba
China
Syria
Iran



Map of Internet Freedom

FREE | PARTLY FREE | NOT FREE | Country not assessed in 2014

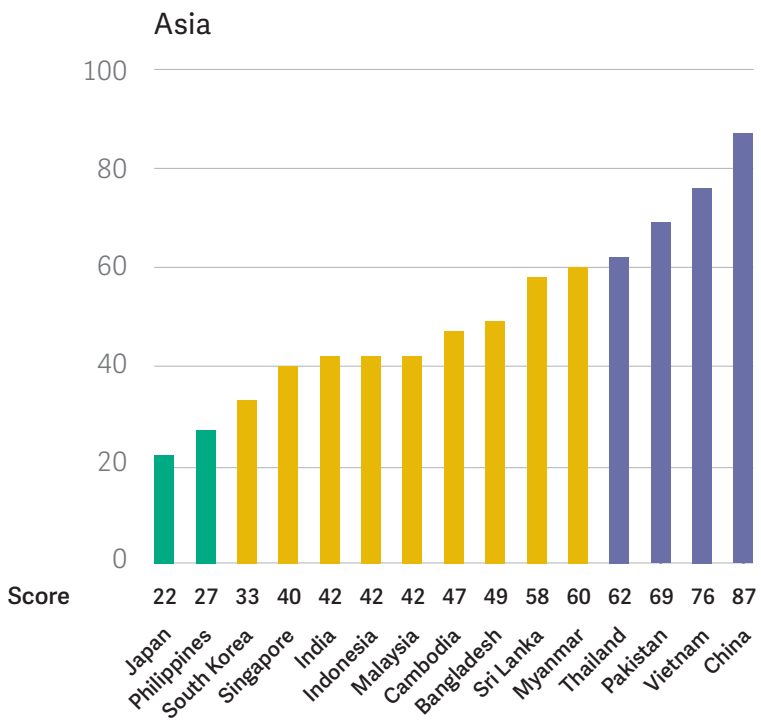


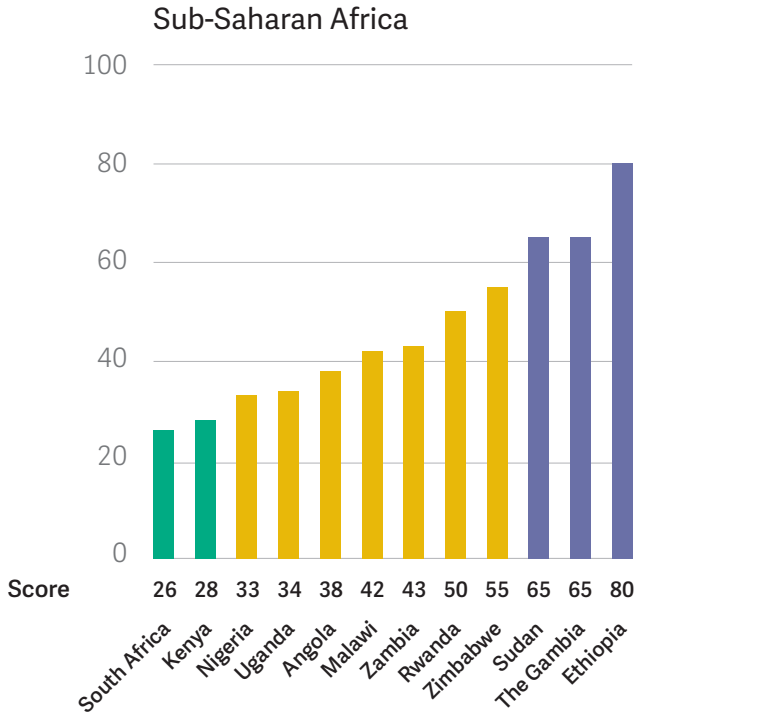
Status	Count
FREE	19
PARTLY FREE	31
NOT FREE	15
Total	**65**

Freedom on the Net 2014 assessed 65 countries around the globe. The project is expected to expand to more countries in the future.

Regional Graphs

Freedom on the Net 2014 covers 65 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

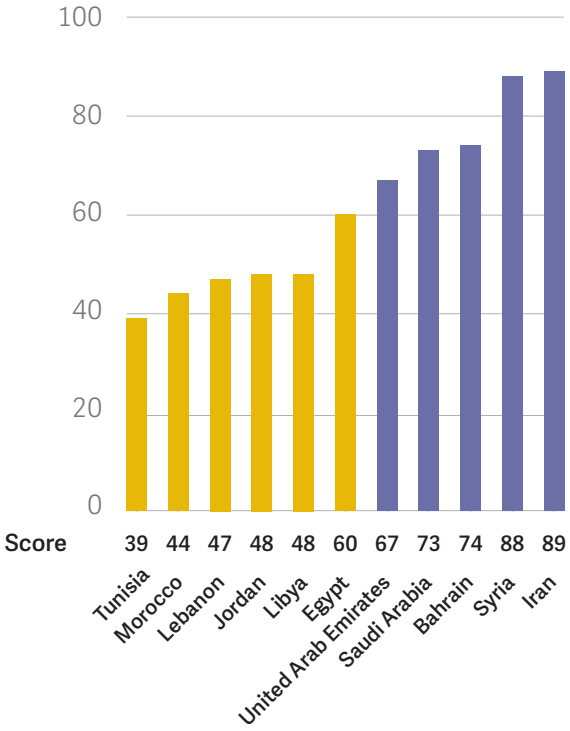




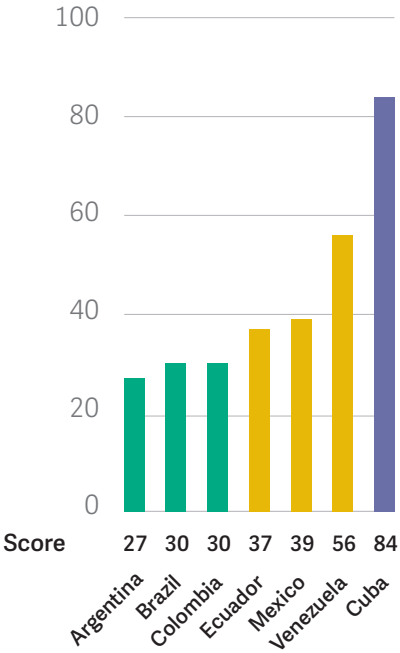
FREE (0–30)
PARTLY FREE (31–60)
NOT FREE (61–100)

0 = Most Free
100 = Least Free

Middle East and North Africa (MENA)

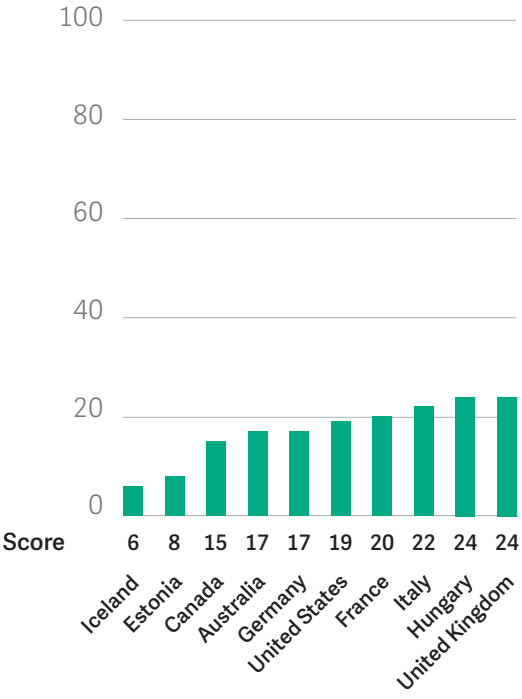


Latin America

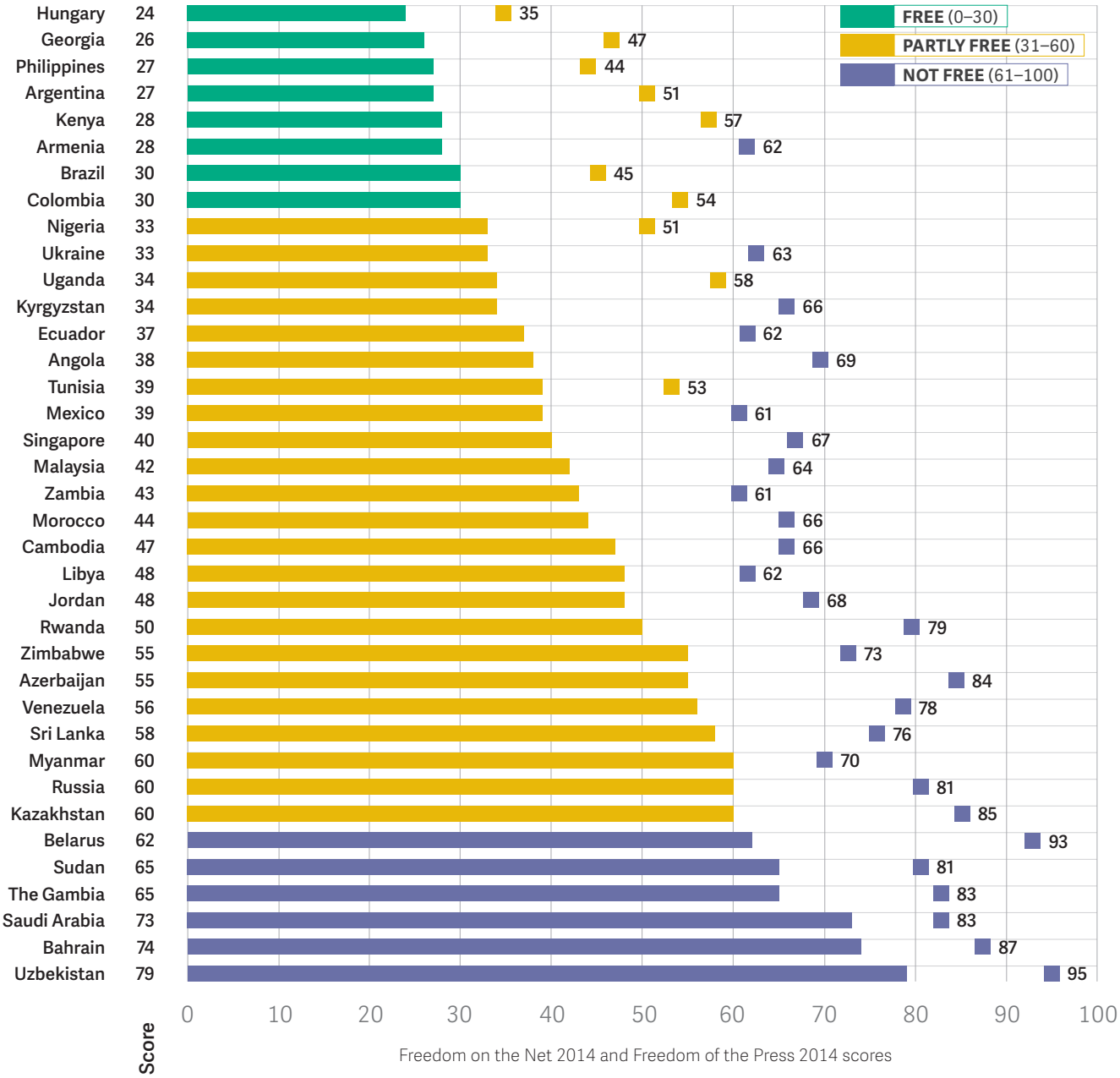


Eurasia

Australia, Canada, European Union, Iceland and United States



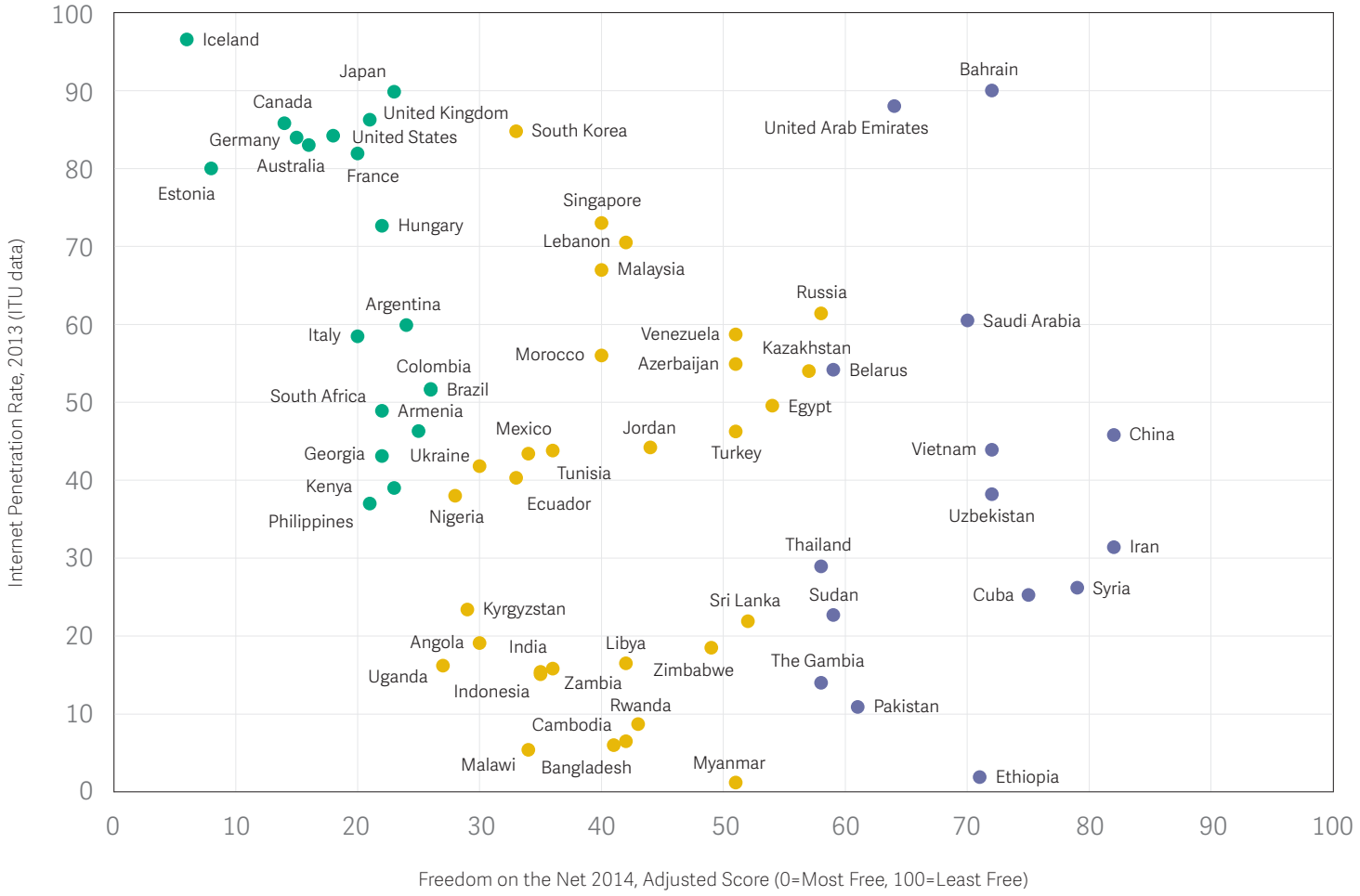
Internet Freedom vs. Press Freedom



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

The figure above shows the 37 countries in this edition with a score difference of 10 points or greater. The bar graph characterizes a country's *Freedom on the Net 2014* score, while the scatterplot (■) represents the country's score in *Freedom of the Press 2014*, which measures media freedom in the broadcast, radio, and print domains. This difference is cause for concern. Pressures that constrain expression in print or broadcast formats have the potential to exert a negative impact, in the short or long term, on the space for online expression.

Internet Freedom vs. Internet Penetration



The figure above depicts the relationship between internet penetration rates and the level of digital media freedom in *Freedom on the Net 2014*. Each point reflects a country's internet penetration rate, as well as its overall performance in the rest of the survey.

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

FREE (0–30)
PARTLY FREE (31–60)
NOT FREE (61–100)

Freedom on the Net 2014: Overview of Score Changes

		Overall				Category Trajectories					
	Country	FOTN 2013	FOTN 2014	Overall Trajectory	FOTN 2014 status	A. Obstacles to Access		B. Limits on Content		C. Violations of User Rights	
Asia	Bangladesh	49	49		Partly Free	12	▲	12		25	▼
	Cambodia	47	47		Partly Free	14		15		18	
	China	86	87	▼	Not Free	19		29		39	▼
	India	47	42	▲	Partly Free	13	▲	10	▲	19	▲
	Indonesia	41	42	▼	Partly Free	11		12	▼	19	
	Japan	22	22		Free	4		7		11	
	Malaysia	44	42	▲	Partly Free	8	▲	14	▲	20	
	Myanmar	62	60	▲	Partly Free	19	▲	16		25	▲
	Pakistan	67	69	▼	Not Free	20		20		29	▼
	Philippines	25	27	▼	Free	10		5		12	▼
	Singapore	*	40	▼	Partly Free	6	*	14	*	20	*
	South Korea	32	33	▼	Partly Free	3		14	▼	16	
	Sri Lanka	58	58		Partly Free	15		20		23	
	Thailand	60	62	▼	Not Free	11	▼	21		30	▼
	Vietnam	75	76	▼	Not Free	14		28		34	▼
Eurasia	Armenia	29	28	▲	Free	7	▲	9		12	
	Azerbaijan	52	55	▼	Partly Free	14	▼	17		24	▼
	Belarus	67	62	▲	Not Free	15	▲	20	▲	27	▲
	Georgia	26	26		Free	8		7		11	
	Kazakhstan	59	60	▼	Partly Free	15		23		22	▼
	Kyrgyzstan	35	34	▲	Partly Free	12		9	▲	13	
	Russia	54	60	▼	Partly Free	10		22	▼	28	▼
	Turkey	49	55	▼	Partly Free	14	▼	18		23	▼
	Ukraine	28	33	▼	Partly Free	8	▼	8	▼	17	▼
	Uzbekistan	78	79	▼	Not Free	20		28		31	▼
Latin America	Argentina	27	27		Free	7	▲	9	▲	11	▼
	Brazil	32	30	▲	Free	7		7	▲	16	▲
	Colombia	*	30		Free	8	*	8	*	14	*
	Cuba	86	84	▲	Not Free	23	▲	28	▲	33	
	Ecuador	37	37		Partly Free	9	▲	11		17	▼
	Mexico	38	39	▼	Partly Free	10	▲	10		19	▼
	Venezuela	53	56	▼	Partly Free	17	▼	18	▼	21	

Decline	▼
Improvement	▲
No change	
New country in 2014	*

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

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

		Overall				Category Trajectories					
	Country	FOTN 2013	FOTN 2014	Overall Trajectory	FOTN 2014 status	A. Obstacles to Access		B. Limits on Content		C. Violations of User Rights	
Middle East & North Africa	Bahrain	72	74	▼	Not Free	12	▼	27	▼	35	
	Egypt	60	60		Partly Free	15		12		33	
	Iran	91	89	▲	Not Free	22		31	▲	36	▲
	Jordan	46	48	▼	Partly Free	12	▲	15	▼	21	▼
	Lebanon	45	47	▼	Partly Free	14		12	▼	21	
	Libya	45	48	▼	Partly Free	18	▼	9		21	▼
	Morocco	42	44	▼	Partly Free	11		10	▼	23	▲
	Saudi Arabia	70	73	▼	Not Free	15	▼	24		34	▼
	Syria	85	88	▼	Not Free	25	▼	26	▼	37	▼
	Tunisia	41	39	▲	Partly Free	11	▲	8		20	▲
	United Arab Emirates	66	67	▼	Not Free	14	▼	22		31	
Sub-Saharan Africa	Angola	34	38	▼	Partly Free	15		7	▼	16	▼
	Ethiopia	79	80	▼	Not Free	23	▼	28		29	
	Gambia, The	*	65	▼	Not Free	19	*	21	*	25	*
	Kenya	28	28		Free	9		7		12	
	Malawi	42	42		Partly Free	16		11		15	
	Nigeria	31	33	▼	Partly Free	10		8		15	▼
	Rwanda	48	50	▼	Partly Free	12		19	▼	19	▼
	South Africa	26	26		Free	7		8		11	
	Sudan	63	65	▼	Not Free	18	▼	19		28	▼
	Uganda	34	34		Partly Free	11		7	▲	16	▼
	Zambia	*	43	▼	Partly Free	12	*	13	*	18	*
	Zimbabwe	54	55	▼	Partly Free	15	▲	15	▼	25	▼
Australia, Canada, European Union, Iceland & United States	Australia	17	17		Free	2		5		10	
	Canada	*	15	▼	Free	3	*	3	*	9	*
	Estonia	9	8	▲	Free	1		3		4	▲
	France	20	20		Free	3	▲	4		13	▼
	Germany	17	17		Free	4		4		9	
	Hungary	23	24	▼	Free	5		8		11	▼
	Iceland	6	6		Free	1		1		4	
	Italy	23	22	▲	Free	4	▲	6		12	
	United Kingdom	23	24	▼	Free	2		6		16	▼
	United States	17	19	▼	Free	4		2	▼	13	▼

Methodology

Freedom on the Net provides analytical reports and numerical ratings for 65 countries worldwide. The countries were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom. The ratings and reports included in this study particularly focus on developments that took place between **May 1, 2013 and May 31, 2014.**

What We Measure

The *Freedom on the Net* index aims to measure each country's level of internet and digital media freedom based on a set of methodology questions described below (see "Checklist of Questions"). Given increasing technological convergence, the index also measures access and openness of other digital means of transmitting information, particularly mobile phones and text messaging services.

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

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

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

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

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

The Scoring Process

The index aims to capture the entire "enabling environment" for internet freedom within each country through a set of 21 methodology questions, divided into three subcategories, which are intended to highlight the vast array of relevant issues. Each individual question is scored on a varying range of points. Assigning numerical points allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. Countries are given a total score from 0 (best) to 100 (worst) as well as a score for each sub-category. Countries scoring between 0 to 30 points overall are regarded as having a "Free" internet and digital media environment; 31 to 60, "Partly Free"; and 61 to 100, "Not Free". An accompanying country report provides narrative detail on the points covered by the methodology questions.

The methodology examines the level of internet freedom through a set of 21 questions and nearly 100 accompanying subpoints, organized into three groupings:

- **Obstacles to Access**—including infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; legal and ownership control over internet and mobile phone access providers.
- **Limits on Content**—including filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
- **Violations of User Rights**—including legal protections and restrictions on online activity; surveillance and limits on privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

The purpose of the subpoints is to guide analysts regarding factors they should consider while evaluating and assigning the score for each methodology question. After researchers submitted their draft scores, Freedom House convened five regional review meetings and numerous international conference calls, attended by Freedom House staff and over 70 local experts, scholars, and civil society representatives from the countries under study. During the meetings, participants reviewed, critiqued, and adjusted the draft scores—based on the set coding guidelines—through careful consideration of events, laws, and practices relevant to each item. After completing the regional and country consultations, Freedom House staff did a final review of all scores to ensure their comparative reliability and integrity.

Checklist of Questions

- Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- A combined score of 0-30=**FREE,** 31-60=**PARTLY FREE**, 61-100=**NOT FREE**.
- Under each question, **a lower number of points is allotted for a more free situation, while a higher number of points is allotted for a less free environment.**
- Unless otherwise indicated, the sub-questions listed are meant to provide guidance as to what issues should be addressed under each methodology question, though not all will apply to every country.

A. Obstacles to Access (0-25 points)

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

    - Does poor infrastructure (electricity, telecommunications, etc.) limit citizens' ability to receive internet in their homes and businesses?
    - To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?
    - To what extent is there internet and mobile phone access, including data connections or satellite?
    - Is there a significant difference between internet and mobile phone penetration and access in rural versus urban areas or across other geographical divisions?
    - 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 socio-economic societal divisions?
    - To what extent are online software, news, and other information available in the main local languages spoken in the country?

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

    - Does the government place limits on the amount of bandwidth that access providers can supply?

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

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

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

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

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

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

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

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

   - Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?
   - Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' interests?
   - Are 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 does the government or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?
    - Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?
    - Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?

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

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

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

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

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

    - To what degree do the government or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?
    - Do authorities issue official guidelines or directives on coverage to online media outlets, blogs, etc., including instructions to marginalize or amplify certain comments or topics for discussion?
    - Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?
    - Does the government employ, or encourage content providers to employ, individuals to post pro-government remarks in online bulletin boards and chat rooms?
    - Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?

6. **Are there economic constraints that negatively impact users' ability to publish content online or online media outlets' ability to remain financially sustainable? *(0-3 points)***

    - Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, email applications, blog hosting platforms, etc.) to be economically viable?
    - Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?
    - Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?

- To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect "net neutrality" with regard to content)?
- To what extent do users have access to free or low-costs blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?

7. **To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content?** ***(0-4 points)***

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

8. **To what extent have individuals successfully used the internet and other ICTs as sources of information and tools for mobilization, particularly regarding political and social issues? To what extent are such mobilization tools available without government restriction?** ***(0-6 points)***

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

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

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

   6a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)
   6b. Cybercafes and other business entities that allow public internet access (0-2 points)
   6c. Mobile phone companies (0-2 points)

   - Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?
   - Are access providers prosecuted for not doing so?
   - Does the state attempt to control access providers through less formal methods, such as codes of conduct?
   - Can the government obtain information about users without a legal process?

7. **Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor?** ***(0–5 points)***

    - Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?
    - Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?
    - Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?
    - Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?

8. **Are websites, governmental and private entities, ICT users, or service providers subject to widespread "technical violence," including cyberattacks, hacking, and other malicious threats?** ***(0-3 points)***

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

Contributors

Freedom House Research Team

Sanja Kelly, Project Director, Freedom on the Net

Mai Truong, Program Officer and Research Analyst (Africa), Freedom on the Net

Madeline Earp, Research Analyst (Asia), Freedom on the Net

Laura Reed, Research Analyst (Eurasia & EU), Freedom on the Net

Adrian Shahbaz, Research Analyst (MENA & EU), Freedom on the Net

Ashley Greco-Stoner, Senior Research Assistant (Latin America), Freedom on the Net

Report Authors and Advisors

Argentina: Eduardo Andres Bertoni, Director, Center for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law, Argentina; Daniela Schnidrig, Research Assistant, CELE

Armenia: Seda Muradyan, Co-Founder, Public Journalism Club NGO, and Armenia Branch Country Director, Institute for War and Peace Reporting

Australia: Dr. Alana Maurushat, Senior Lecturer, Faculty of Law, and Co-Director, Cyberspace Law and Policy Community, The University of New South Wales

Azerbaijan: Arzu Geybullayeva, freelance blogger and journalist

Bangladesh: Dr. Faheem Hussain, Assistant Professor, Department of Technology and Society, State University of New York (SUNY) Korea

Brazil: Carolina Rossini, Vice President, International Policy, at Public Knowledge; Fabrício Bertini Pasquot Polido, Professor, Law School of Federal University of Minas Gerais, and Head of Center for International Studies on Internet, Innovation and Intellectual Property – GNet

Cambodia: Sopheap Chak, Executive Director, Cambodian Center for Human Rights, and human rights blogger

Canada: Michael Geist, Canada Research Chair in Internet and E-commerce Law, University of Ottawa

China: Madeline Earp, Research Analyst, Freedom on the Net, Freedom House

Colombia: Carlos Cortés, Media Policy Consultant, and Researcher of the Center for Freedom of Expression Studies (CELE) at Palermo University, Argentina

Cuba: Ernesto Hernández Busto, Cuban journalist and writer, Barcelona

Estonia: Linnar Viik, Lecturer, Board Member, Estonian IT College

France: Jean-Loup Richet, Researcher, University of Nantes

Georgia: Teona Turashvili, Analyst at Institute for Development of Freedom of Information (IDFI), Georgia

Germany: Philipp Otto, Digital Strategist and Editor in Chief, iRights.info, Founder, iRights.Lab think tank, iRights.Media publishing house; Henning Lahmann, Research Assistant, iRights.Lab.

Hungary: Borbála Tóth, Independent Researcher

Iceland: Caroline Nellemann, Independent Consultant and Specialist in Digital Media and Civic Engagement

India: Chinmayi Arun, Research Director, Center for Communication Governance at National Law University, Delhi, Sarvjeet Singh, Project Manager and Research Fellow, Centre for Communication Governance, Parul Sharma, Student, B.A., LL.B. (Hons.), National Law University, Medha Vikram, Student, B.A., LL.B. (Hons.), National Law University

Indonesia: Indriaswati Dyah Saptaningrum, Executive Director, ELSAM (The Institute for Policy Research and Advocacy)

Iran: Mahmood Enayat, Director, Small Media

Italy: Giampiero Giacomello, Associate Professor of International Relations, University of Bologna

Japan: Dr. Leslie M. Tkach-Kawasaki, Associate Professor, University of Tsukuba

Jordan: Abeer al-Najjar, Assistant Professor of Journalism and Media Studies, American University of Sharjah

Kazakhstan: Adil Nurmakov, Senior Lecturer, KIMEP University

Kenya: Grace Githaiga, Associate, Kenya ICT Action Network (KICTANet)

Kyrgyzstan: Artem Goriyanov, IT Programs Director, Public Foundation CIIP

Lebanon: Dr. Jad Melki, Assistant Professor of Journalism and Media Studies and Director, Media Studies Program, American University of Beirut

Libya: Danya Bashir Hobba, Ambassador, One Young World

Malawi: Gregory Gondwe, Bureau Chief, Times Media Group, Malawi

Malaysia: K. Kabilan, Managing Editor, The Ant Daily

Mexico: Jorge Luis Sierra, Director, Knight International Journalism Fellowships, International Center for Journalists

Morocco: Bouziane Zaid, Assistant Professor of Media and Communication, Al Akhawayn University in Ifrane

Myanmar: Min Zin, PhD Candidate, Department of Political Science, University of California, Berkeley, and Contributor, Foreign Policy Democracy Lab channel

Nigeria: 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria

Pakistan: Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan, Lawyer and Internet Freedom Activist

Philippines: Jacques D.M. Gimeno, Assistant Professor, Communication Research Department, University of the Philippines-Diliman

Saudi Arabia: Abeer Allam, former Riyadh-based Correspondent, Financial Times

Singapore: Cherian George, Associate Professor, School of Communication, Hong Kong Baptist University

South Africa: Alan Finlay, Independent Consultant, Open Research

South Korea: Dr. Yenn Lee, Research Skills Trainer/ Coordinator, School of Oriental and African Studies, University of London

Sri Lanka: Nigel V. Nugawela, Independent writer and researcher

Syria: Dlshad Othman, ICT Specialist, Information Safety & Capacity Project (ISC)

Turkey: Yaman Akdeniz, Professor of Law, Istanbul Bilgi University and Founder of Cyber-Rights.org

Uganda: Lillian Nalwoga, Policy Officer, Collaboration on International ICT Policy in East and Southern Africa (CIPESA), President, Internet Society Uganda Chapter

Ukraine: Tetyana Lokot, Doctoral Student and Researcher, Philip Merrill College of Journalism, University of Maryland, College Park and Coeditor, RuNet Echo at Global Voices

United Kingdom: LSE Media Policy Project, London School of Economics and Political Science

United States: Emily Barabas, Policy Analyst, Center for Democracy and Technology

Uzbekistan: Zhanna Hördegen, Independent Consultant and Research Associate at the University Research Priority Program Asia and Europe, University of Zurich

Venezuela: Raisa Urribarri, Director, Communications Lab for Teaching, Research and Community Extension (LIESR) at the University of Los Andes.

Zambia: Brenda Nglazi Zulu, Founder and Director, Africa Interactive Media and Zambian Bloggers Network

The analysts for the reports on Angola, Bahrain, Belarus, Ecuador, Egypt, Ethiopia, The Gambia, Russia, Rwanda, Thailand, Tunisia, Sudan, United Arab Emirates, Vietnam and Zimbabwe are independent internet researchers who have requested to remain anonymous. Xiao Qiang, founder and chief editor of China Digital Times, and adjunct professor of the School of Information, University of California at Berkeley, was an advisor for the China report.

The internet is a crucial medium not just for personal communication or news and information, but for political participation and civic engagement. The struggle for internet freedom is consequently inseparable from the struggle for freedom of every kind.

Design: Designlounge, Inc., New York

Freedom House

http://www.freedomhouse.org

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 D.C. 20036

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

www.freedomhouse.org

202.296.5101
info@freedomhouse.org