Silencing the Messenger:
Communication Apps under Pressure

November 2016

Freedom House

FREEDOM ON THE NET 2016

Freedom on the Net 2016

Table of Contents

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

This booklet is a summary of findings for the 2016 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

A Bahraini woman uses a mobile phone to take photos during clashes with riot police in Sitra, south of the capital Manama, January 2016.

Photo credit: Mohammed al-Shaikh/AFP/Getty Images

Freedom House

Silencing the Messenger: Communication Apps under Pressure

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

Internet freedom has declined for the sixth consecutive year, with more governments than ever before targeting social media and communication apps as a means of halting the rapid dissemination of information, particularly during antigovernment protests.

Public-facing social media platforms like Facebook and Twitter have been subject to growing censorship for several years, but in a new trend, governments increasingly target messaging and voice communication apps such as WhatsApp and Telegram. These services are able to spread information and connect users quickly and securely, making it more difficult for authorities to control the information landscape or conduct surveillance.

The increased controls show the importance of social media and online communication for advancing political freedom and social justice. It is no coincidence that the tools at the center of the current crackdown have been widely used to hold governments accountable and facilitate uncensored conversations. Authorities in several countries have even resorted to shutting down all internet access at politically contentious times, solely to prevent users from disseminating information through social media and communication apps, with untold social, commercial, and humanitarian consequences.

Some communication apps face restrictions due to their encryption features, which make it extremely difficult for authorities to obtain user data, even for the legitimate purposes of law enforcement and national security. Online voice and video calling apps like Skype have also come under pressure for more mundane reasons. They are now restricted in several countries to protect the revenue of national telecommunications firms, as users were turning to the new services instead of making calls through fixed-line or mobile telephony.

Other key trends

Social media users face unprecedented penalties: In addition to restricting access to social media and communication apps, state authorities more frequently imprison users for their posts and the content of their messages, creating a chilling effect among others who write on controversial topics. Users in some countries were put behind bars for simply "liking" offending material on Facebook, or for not denouncing critical messages sent to them by others. Offenses that led to arrests ranged from mocking the king's pet dog in Thailand to "spreading atheism" in Saudi Arabia. The number of countries where such arrests occur has increased by over 50 percent since 2013.

In a new trend, governments increasingly target messaging and voice communication apps such as WhatsApp and Telegram.

Governments censor more diverse content: Governments have expanded censorship to cover a growing diversity of topics and online activities. Sites and pages through which people initiate digital petitions

or calls for protests were censored in more countries than before, as were websites and online news outlets that promote the views of political opposition groups. Content and websites dealing with LGBTI (lesbian, gay, bisexual, transgender, and intersex) issues were also increasingly blocked or taken down on moral grounds. Censorship of images—as opposed to the written word—has intensified, likely due to the ease with which users can now share them, and the fact that they often serve as compelling evidence of official wrongdoing.

Security measures threaten free speech and privacy: In an effort to boost their national security and law enforcement powers, a number of governments have passed new laws that limit privacy and authorize broad surveillance. This trend was present in both democratic and nondemocratic countries, and often led to political debates about the extent to which governments should have backdoor access to encrypted communications. The most worrisome examples, however, were observed in authoritarian countries, where governments used antiterrorism laws to prosecute users for simply writing about democracy, religion, or human rights.

The number of countries where arrests for online posts occur has increased by over 50 percent since 2013.

Online activism reaches new heights: The internet remained a key tool in the fight for better governance, human rights, and transparency. In over two-thirds of the countries in this study, internet-based activism has led to some sort of tangible outcome, from the defeat of a restrictive legislative proposal to the exposure of corruption through citizen journalism. During the year, for example, internet freedom activists in Nigeria helped thwart a bill that would have limited social media activity, while a WhatsApp group in Syria helped save innocent lives by warning civilians of impending air raids.

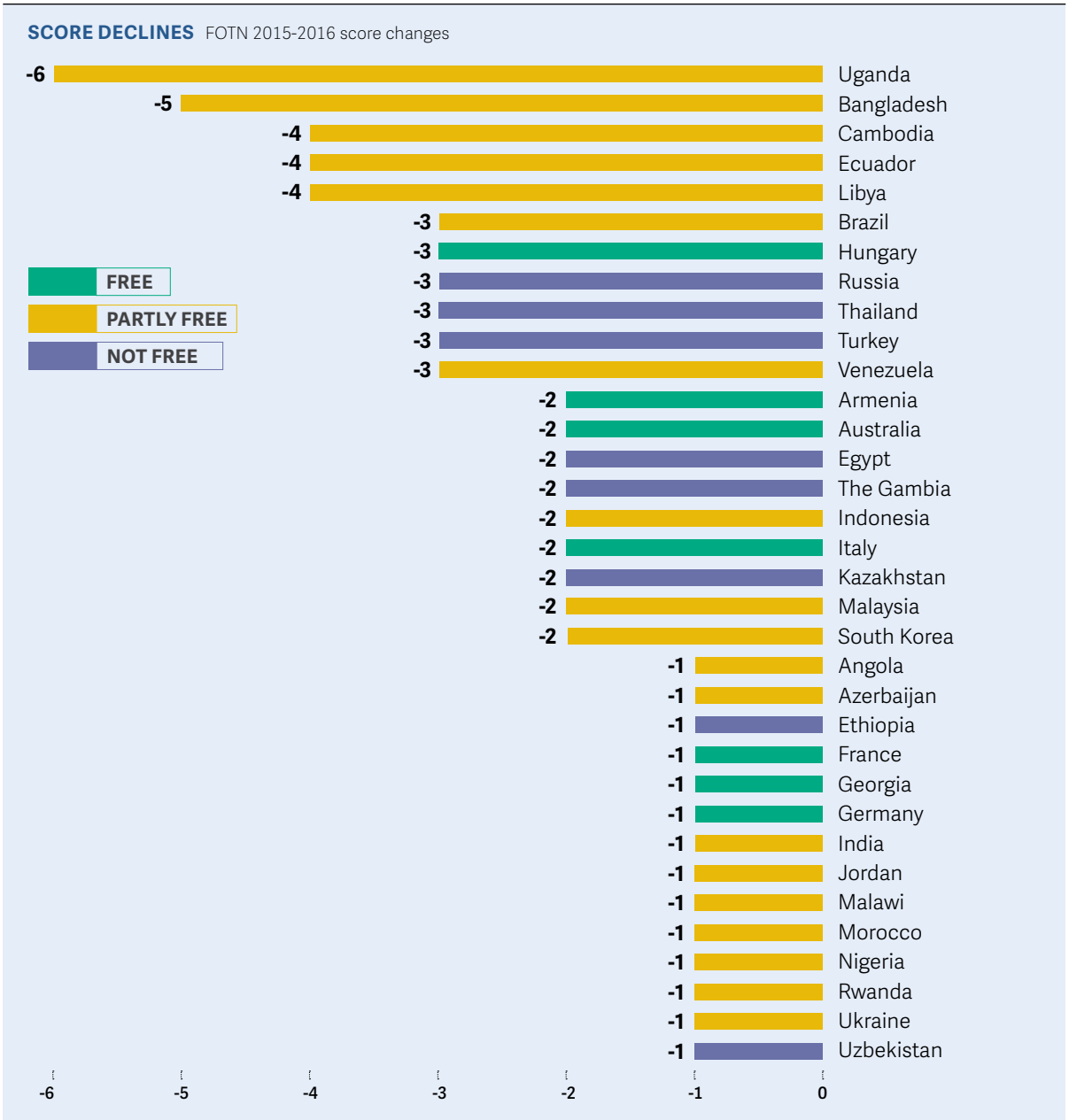
Tracking the global decline

Freedom on the Net is a comprehensive study of internet freedom in 65 countries around the globe, covering 88 percent of the world's internet users. It tracks improvements and declines in governments' policies and practices each year, and the countries included in the study are selected to represent diverse geographical regions and types of polity. This report, the seventh in its series, focuses on developments that occurred between June 2015 and May 2016, although some more recent events are included in individual country narratives. More than 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, 34 have been on a negative trajectory since June 2015. The steepest declines were in Uganda, Bangladesh, Cambodia, Ecuador, and Libya. In Uganda, the government made a concerted effort to restrict internet freedom in the run-up to the presidential election and inauguration in the first half of 2016, blocking social media platforms and communication services such as Facebook, Twitter, and WhatsApp for several days. In Bangladesh, religious extremists claimed responsibility for the murders of a blogger and the founder of an LGBTI magazine with a community of online supporters. And Cambodia passed an overly broad telecommunications law that put the industry under government control, to the detriment of service providers and user privacy. Separately, Cambodian police arrested several people for their Facebook posts, including one about a border dispute with Vietnam.

China was the year's worst abuser of internet freedom. The Chinese government's crackdown on free expression under President Xi Jinping's "information security" policy is taking its toll on the digital activists who have traditionally fought back against censorship and surveillance. Dozens of prosecutions related to online expression have increased self-censorship, as have legal restrictions introduced in 2015. A criminal law amendment added seven-year prison terms for spreading rumors on social media (a charge often used against those who criticize the authorities), while some users belonging to minority religious groups were imprisoned simply for watching religious videos on their mobile phones. The London-based magazine *Economist* and the Hong Kong–based *South China Morning Post* were newly blocked in mainland China, as were articles and commentaries about sensitive events including a deadly chemical blast in Tianjin in 2015.

Turkey and Brazil were downgraded in their internet freedom status. In Brazil, which slipped from Free to Partly Free, courts imposed temporary blocks on WhatsApp for its failure to turn over user data in criminal investigations, showing little respect for the principles of proportionality and necessity. Moreover,



at least two bloggers were killed after reporting on local corruption. Turkey, whose internet freedom environment has been deteriorating for a number of years, dropped into the Not Free category amid multiple blockings of social media platforms and prosecutions of users, most often for offenses related to criticism of the authorities or religion. These restrictions continued to escalate following the failed coup in July 2016, in spite of the crucial role that social media and communication apps—most notably FaceTime—played in mobilizing citizens against the coup.

Just 14 countries registered overall improvements. In most cases, their gains were quite modest. Users in Zambia faced fewer restrictions on online content compared with the previous few years, when at least two critical news outlets were blocked. South Africa registered an improvement due to the success of online activists in using the internet to promote societal change and diversifying online content, rather than any positive government actions. Digital activism also flourished in Sri Lanka as censorship and rights violations continued to decline under President Maithripala Sirisena's administration. And the United States registered a slight improvement to reflect the passage of the USA Freedom Act, which puts some limits on bulk collection of telecommunications metadata and establishes several other privacy protections.

Major Developments

Social Media and Communication Tools under Assault

In the past year, social media platforms, communication apps, and their users faced greater threats than ever before in an apparent backlash against growing citizen engagement, particularly during politically sensitive times. Of the 65 countries assessed, governments in 24 impeded access to social media and communication tools, up from 15 the previous year. Governments in 15 countries temporarily shut down access to the entire internet or mobile phone networks, sometimes solely to prevent users from disseminating information through social media. Meanwhile, the crackdown on users for their activities on social media or messaging apps reached new heights as arrests and punishments intensified.

Governments in 24 countries impeded access to social media and communication tools, up from 15 the previous year.

New restrictions on messaging apps and internet-based calls

In a new development, the most routinely targeted tools this year were instant messaging and calling platforms, with restrictions often imposed during times of protests or due to national security concerns. Governments singled out these apps for blocking due to two important features: encryption, which protects the content of users' communications from interception, and text or audiovisual calling functions, which have eroded the business model and profit margins of traditional telecommunications companies.

Whatever the justification, restrictions on social media and internet-based communication tools threaten to infringe on users' fundamental right to access the internet. In a landmark resolution passed in July 2016, the UN Human Rights Council condemned state-sponsored disruptions to internet access and the free flow of information online.

WhatsApp faced the most restrictions, with 12 out of 65 countries blocking the entire service or disabling certain features, affecting millions of its one billion users worldwide. Telegram, Viber, Facebook Messenger, LINE, IMO, and Google Hangouts were also regularly blocked. Ten countries restricted access to platforms that enable voice and video calling over the internet, such as Skype and FaceTime.

Nearly ubiquitous among internet and mobile phone users, these communication platforms have become essential to the way we connect with the world. Incidents of blocking have had far-reaching effects, preventing family members from checking in during a crisis, activists from documenting police abuses during a protest, and individuals from communicating affordably with social and professional contacts abroad.

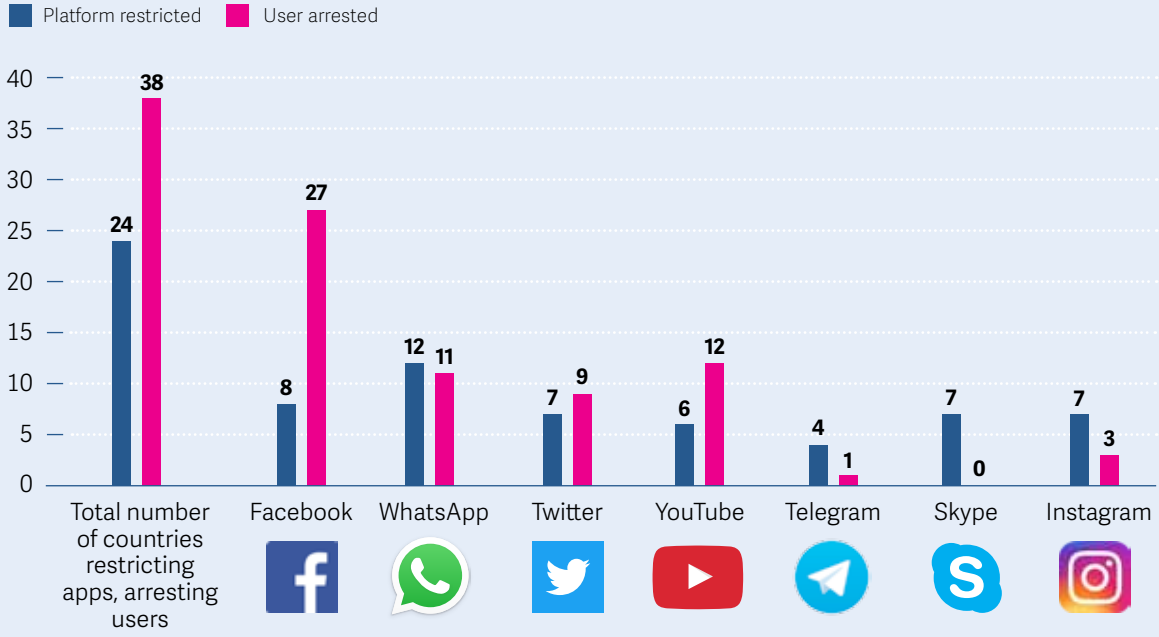
While all users are adversely affected by restrictions, the harm is often disproportionately felt by marginalized communities and minority groups, who are more likely to be cut off from critical information sources and the ability to advocate for their rights. In the United Arab Emirates (UAE), for example, where migrant workers and other noncitizens make up 88 percent of the population, blocks on communication tools have made it difficult for these individuals to organize or seek support from their home countries.

App blocking aimed at protests, expressions of dissent

Authoritarian regimes most frequently restricted communication apps to prevent or quell antigovernment protests, as they have become indispensable for sharing information on demonstrations and organizing participants in real time. In Ethiopia, ongoing protests that began in November 2015 in response to the government's marginalization of the Oromo people have

NUMBER OF COUNTRIES WHERE POPULAR APPS WERE BLOCKED OR USERS ARRESTED

WhatsApp was blocked more than any other tool, while Facebook users were arrested for posting political, social, or religious content in 27 countries.



been met with periodic blocks on services including WhatsApp, Facebook Messenger, and Twitter. In Bahrain, Telegram was blocked for several days around the anniversary of the February 14, 2011, "Day of Rage" protests, likely to quash any plans for renewed demonstrations.

In Bangladesh, the authorities ordered the blocking of platforms including Facebook Messenger, WhatsApp, and Viber to prevent potential protests following a Supreme Court ruling in November that upheld death sentences for two political leaders convicted of war crimes. The longest block lasted 22 days. In Uganda, officials directed internet service providers to block WhatsApp, Facebook, and Twitter for several days during the presidential election period in February 2016 and again in the run-up to the reelected incumbent's inauguration in May. In both instances, the unprecedented blocking worked to silence citizens' discontent with the president's 30-year grip on power and their efforts to report on the ruling party's notorious electoral intimidation tactics.

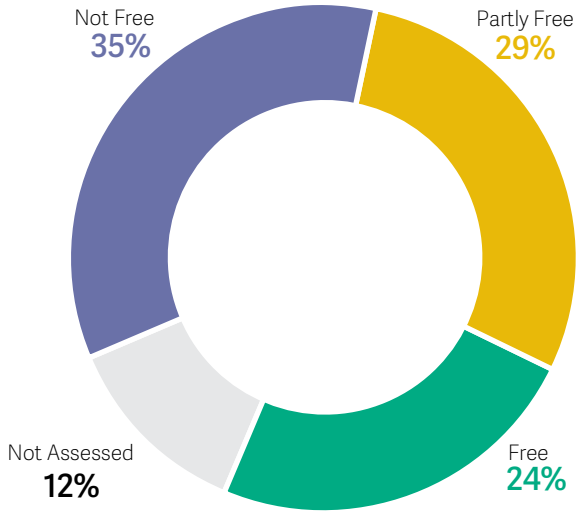
New security and encryption features also trigger blocking

Governments increasingly imposed restrictions on internet-based messaging and calling services due to their strong privacy and security features, which have attracted many users amid growing concerns about surveillance worldwide.

Telegram was blocked in China after the authorities learned of its popularity among human rights lawyers.

GLOBAL INTERNET POPULATION BY 2016 FOTN STATUS

FOTN assesses 88 percent of the world's internet user population.



In many countries, individuals are using messaging apps as private social networks where they can enjoy greater freedom of expression than on more established, public-facing social networks such as Facebook and Twitter. New messaging and calling apps also provide greater anonymity than conventional voice and SMS services that can be tracked due to SIM-card registration requirements, and several offer end-to-end encryption that prevents wiretapping and interception.

Activists and human rights defenders in repressive countries protect their communications by convening on WhatsApp, Viber, and Telegram to share sensitive information, conduct advocacy campaigns, or organize protests. Journalists in Turkey, for example, have established new distribution networks for their reporting via group channels on WhatsApp to avert censorship.

The same security features that appeal to users of the new platforms have brought them into conflict with governments in both democratic and authoritarian countries. In Brazil in 2015 and 2016, regional courts ordered a block on WhatsApp three times after it failed to turn over encrypted communications to local authorities during criminal investigations. On all three occasions, WhatsApp's parent company, Facebook, insisted that it did not have access to the information in question, since WhatsApp does not store the content of users' communications. Nevertheless, the judges chose to penalize not just the company, but also Brazil's 100 million WhatsApp users.

Authoritarian regimes targeted Telegram for its "secret chat" mode, which allows messages to self-delete after a period of time. The platform was blocked in China after the authorities learned of its popularity among human rights lawyers, joining a long list of other international communication apps that are unavailable to Chinese users. State-run news outlets in the country accused Telegram of aiding activists in "attacks on the [Communist] Party and government." Iran also targeted Telegram, blocking it for a week in October 2015 when it refused to aid officials' surveillance and censorship efforts. In May 2016, Iran's Supreme Council on Cyberspace ordered Telegram to host all data on Iranian users inside the country or face blocking.

Market threats to national telecoms lead to backlash

Internet-based messaging and calling platforms faced increasing restrictions from governments seeking to protect their countries' major state-owned or private telecommunications companies. Given the rising popularity of new communication services over the past decade, telecoms in some markets have become concerned about the future economic viability of their traditional text and voice services, particularly when the new competitors are not subject to the same regulatory obligations and fees.

Typically free to download, messaging platforms such as WhatsApp, Telegram, and Facebook Messenger have proliferated in emerging markets, where the advent of low-cost, internet-enabled mobile devices and smartphones have made sending messages, photos, and even videos via online tools much more affordable than traditional SMS, for which telecom carriers charge a variable rate per message. Indeed, app-based mobile messaging has surpassed SMS texting worldwide since at least 2013.

Similarly, Voice over Internet Protocol (VoIP) and internet-based video calling services such as Skype, Google Hangouts, and Apple's FaceTime have signifi-

cantly reduced the cost of real-time audio and visual communication for users, resulting in the decreased use of traditional phone services that charge by the minute. Though telecom companies still profit from the data used by internet-based platforms, continual improvements in network infrastructure have only made data plans cheaper, threatening to leave traditional voice and SMS services further behind.

One of the first market-related restrictions on internet-based communication services was imposed by the American telecommunications company AT&T in 2007, when it partnered with Apple to become the sole mobile provider for the first iPhone and subsequently banned VoIP applications that could make calls using a wireless data connection. Google's Voice app was consequently rejected by the iPhone's app store, and Skype developed a version of its platform that only allowed iPhone users to make calls when connected to a Wi-Fi network. Under pressure from the Federal Communications Commission (FCC), AT&T changed course in 2009, setting a positive precedent and providing users with more freedom to choose from a suite of services based on quality and affordability.

In the past year, restrictions to protect market interests escalated most prominently in the Middle East and North Africa. The UAE had been an early mover, requiring VoIP services to obtain a license to operate as a telecom provider and subsequently blocking both the voice and video calling features of Skype, WhatsApp, and Facebook Messenger in 2014, in an effort to protect the profits of state-owned telecom companies. Most recently, Snapchat's calling function was disabled in April 2016. While circumvention tools such as virtual private networks (VPNs) were widely used to bypass the blocks, the government cracked down in July 2016, adopting amendments to the Cybercrime Law that penalize the "illegal" use of VPNs with temporary imprisonment, fines of between US$136,000 and US$545,000, or both.

Morocco's telecommunications regulator issued a directive in January 2016 that suspended all internet calling services over mobile networks, citing previously unenforced licensing requirements under the 2004 telecommunications law. The order seemed heavily influenced by the UAE's Etisalat, which purchased a majority stake in Maroc Telecom, the country's largest operator, in 2014. In Egypt, where long-distance VoIP calls on Skype have been blocked since 2010, voice calling features on WhatsApp and Viber have reportedly been inaccessible since October 2015. The calling functions of popular platforms were also disabled in Saudi Arabia, while Apple has been forced to sell its iPhone in the kingdom without the built-in FaceTime app.

A Turkish man was handed a one-year suspended sentence for this meme juxtaposing President Reçep Tayyip Erdogan and a character from the Lord of the Rings films. In determining whether or not the image insulted the president, the judge assembled a panel of film experts. Another user is facing up to two years in prison for reposting the same meme.

Pressure to regulate mobile communication services in the past year threatened to impede access to such platforms in other regions, particularly sub-Saharan Africa, where mobile internet use has been growing rapidly. In Kenya, Nigeria, South Africa, and Zimbabwe, private telecommunications companies lobbied governments to regulate internet-based messaging and voice calling platforms such as Skype and WhatsApp, citing concerns over their profits. Meanwhile, Ethiopia's single telecommunications provider, state-owned

Since June 2015, police in 38 countries arrested individuals for their activities on social media.

EthioTelecom, announced plans in April 2016 to introduce a new pricing scheme for mobile users of popular communication applications. Companies in the European Union (EU) pushed EU officials throughout 2016 to regulate new communication services, calling for a "level playing field" that subjects messaging and calling platforms to the same regulatory framework, licensing fees, and law enforcement access requirements as traditional telecoms.

Social media users face unprecedented penalties

While many governments attempted to restrict access to social media and communication platforms, far more turned to traditional law enforcement methods to punish and deter users. Since June 2015, police in a remarkable 38 countries arrested individuals for their activities on social media, compared with 21 countries where people were arrested for content published on news sites or blogs. The rising penetration of social networks in repressive societies has enabled discussion and information sharing on issues that governments deem sensitive, resulting in arrests of journalists, politicians, activists, and ordinary citizens who may not be aware that they are crossing redlines.

A Saudi court sentenced an individual to 10 years in prison and 2,000 lashes for spreading atheism on Twitter.

Dramatic sentences for social media 'crimes'

Social media users were prosecuted for a range of alleged crimes during the coverage period. Some supposed offenses were quite petty, illustrating both the sensitivity of some regimes and the broad discretion given to police and prosecutors under applicable laws. Lebanon's bureau of cybercrimes interrogated a Facebook user for criticizing a Lebanese singer, while soldiers in the UAE were arrested for disrespecting the army after they shared a video of themselves recreating a popular dance craze in their uniforms.

While severe punishments for online speech are not new, their application to social media activities that many people engage in daily was a cause for serious concern. In February 2016, a Saudi court sentenced an individual to 10 years in prison and 2,000 lashes for allegedly spreading atheism in 600 tweets. In the harshest examples of the coverage period, military courts in Thailand issued 60- and 56-year sentences in separate cases involving Facebook posts that were deemed critical of the monarchy in August 2015, though they were reduced to 30 and 28 years after the defendants pleaded guilty. While sentences like these may not cause people to stop using social media entirely, they are likely to encourage self-censorship on sensitive topics, robbing the technology of its potential for galvanizing social and political change.

Many detentions were justified under criminal laws penalizing defamation or insult, but they often aimed to suppress information in the public interest. In Morocco, YouTube footage of a man lifting asphalt barehanded from a local road led to his arrest for allegedly defaming the official responsible for the poor construction.

Users punished for their connections and readership

One goal of social media is to allow users to share content with a wide circle of connections. Police in some countries seem determined to undermine that goal, specifically pursuing individuals whose content goes viral. In Zimbabwe, Pastor Evan Mawarire was arrested in July 2016 after his YouTube videos criticizing the country's leadership sparked the #ThisFlag social media campaign and inspired nationwide protests. Elsewhere, charges often multiplied as content was passed along: in November 2015, 17 people in Hungary were charged with defamation for sharing a Facebook post that questioned the legitimacy of the mayor of Siófok's financial dealings.

In a disturbing development, defendants whose content failed to spread widely were nevertheless punished as a warning to others. In Russia, mechanical engineer Andrey Bubeyev was sentenced to two years in prison in May 2016 for reposting material that identified the Russian-occupied Crimean Peninsula as part of Ukraine on the social network VKontakte. He shared the information with just 12 contacts.

Authorities in other cases scoured social media for a pretext to charge specific individuals, or were so intent on suppressing certain content that identifying the correct defendant was of secondary importance. In Ethiopia, charges against an opposition politician and student protesters principally cited evidence gleaned from social media. Pseudonymous accounts offered limited protection and raised the risk of mistaken identity. A man in Uganda was charged on suspicion of operating the popular Facebook page Tom Voltaire Okwalinga, but he denied being responsible for the page, which frequently accused senior leaders of corruption

and incompetence. Some people were held responsible for posts clearly made by others. At least three criminal charges were filed in India against the administrators of WhatsApp groups based on offensive or antireligious comments shared by other group members.

A number of users were apparently targeted only to punish their associates. In Thailand, Patnaree Chankij, the mother of an activist who opposes Thailand's military government, was charged with insulting the monarchy based on a private, one-word acknowledgement she sent in reply to a Facebook Messenger post from her son's friend; police said she failed to criticize or take action against the antiroyalist sentiment in the post, instead replying "yes" or "I see." Patnaree told journalists that the charge was in reprisal for her son's activities. In China, police detained the local relatives of at least three overseas journalists and bloggers who produce online content that the Chinese government perceives as critical.

Governments Censor More Diverse Content

This year featured new trends in the type of content that attracted official censorship. Posts related to the LGBTI community, political opposition, digital activism, and satire resulted in blocking, takedowns, or arrests for the first time in many settings. Authorities also demonstrated an increasing wariness of the power of images on today's internet.

A longer roster of forbidden topics

Attempts to censor LGBTI content were observed in 18 countries, up from 14 in 2015, as more individuals and groups sought to use digital tools to connect and share resources, sometimes in defiance of local laws or religious beliefs. In July 2016, an LGBTI group reported that Azerbaijan's national domain-name registrar was declining to register website domains like lgbt.az. In Indonesia, the information ministry asked the LINE messaging platform to remove emojis with gay or lesbian themes from its online store. Also in 2016, South Korean regulators told the Naver web portal to exercise "restraint" after it linked to an online gay drama. At least 13 countries blocked content serving the LGBTI community on moral grounds, including Saudi Arabia and Sudan. Turkish authorities systematically blocked the most popular LGBTI websites over several weeks in mid-2015.

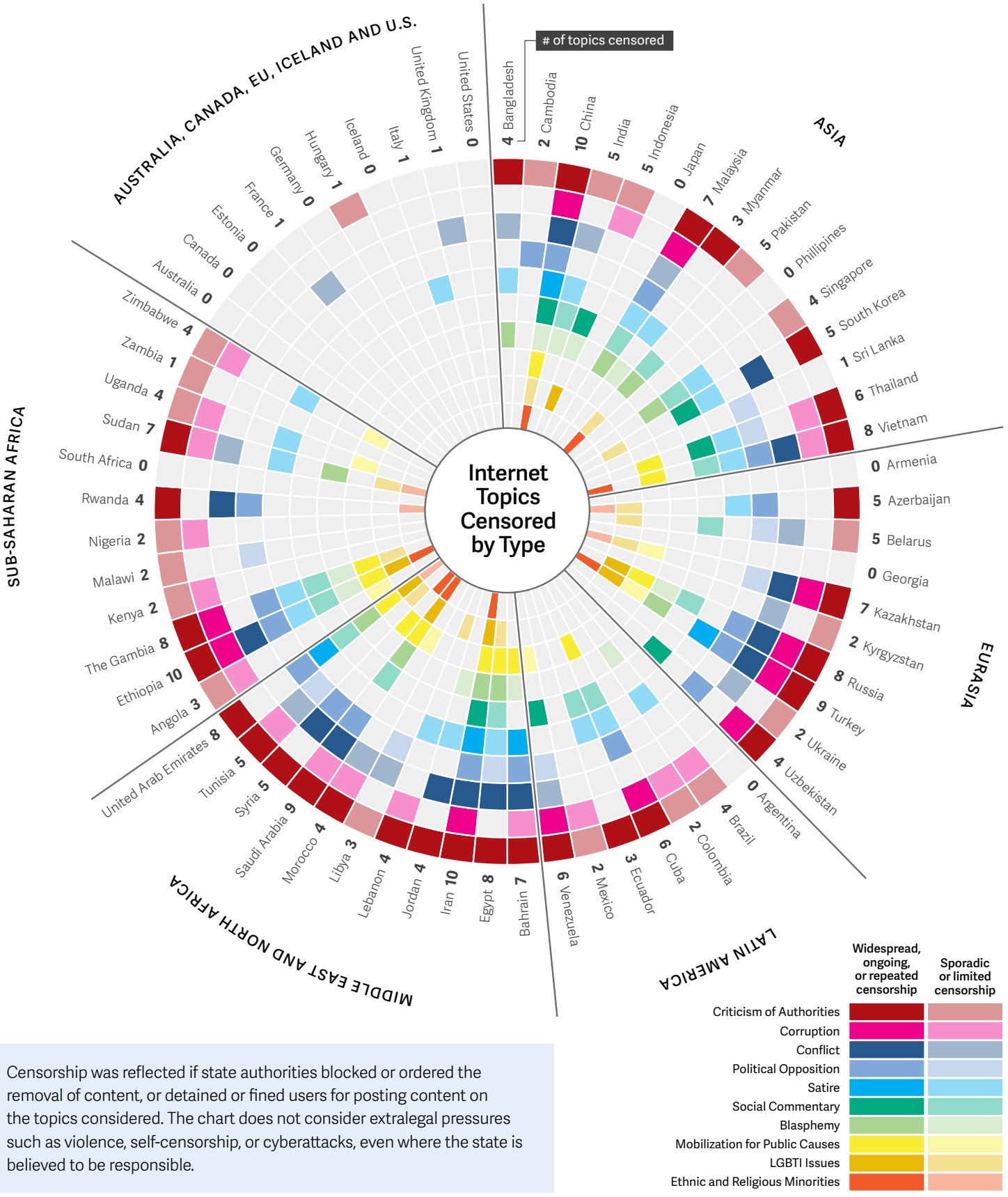
Content related to political opposition was subject to censorship in 26 countries, an increase from 23 in 2015. A court in Kazakhstan ordered an opposition-affiliated magazine to shutter its Facebook page along with its print edition in October 2015. In Bahrain, prosecutors questioned Sheikh Ali Salman, leader of the country's largest political organization, for allegedly tweeting about democracy, even though he was already imprisoned; police are now investigating who continues to operate the account.

A 22 year-old student in Egypt was sentenced to three years in prison for posting this photo depicting President Abdel Fattah al-Sisi with Mickey Mouse ears on Facebook.

Digital activism, including petitions, campaigns for social or political action, and protests, were subject to censorship in 20 countries in *Freedom on the Net*, up from 16 in 2015. Campaigns using smartphones or social media can appear dangerous because they are particularly effective at reaching young people. In The Gambia, a Facebook post calling on young people to join peaceful protests disappeared in April 2016 and was replaced with a warning to abide by the law; the protest organizer left the country, citing death threats. Because online mobilization amplifies discontent, authorities in many countries sought to shut it down even when the issues at stake were local. In Kazakhstan, two activists were arrested in May 2016 for planning on social media to attend land-reform protests scheduled to take place the next day.

Authorities in 26 of the 65 countries assessed, up from 23 in 2015, tried to suppress satire, which often skewered public officials. A poet in Myanmar was charged in November 2015 for posting a satirical poem on Facebook that described a newlywed's dismay at discovering a tattoo of the president on her husband's genitals.

CENSORED TOPICS BY COUNTRY



Censorship was reflected if state authorities blocked or ordered the removal of content, or detained or fined users for posting content on the topics considered. The chart does not consider extralegal pressures such as violence, self-censorship, or cyberattacks, even where the state is believed to be responsible.

Other topics that have long been subject to censorship remained in authorities' crosshairs this year:

- **Criticism of the authorities** was censored in 49 out of 65 countries, two more than in the previous year. In Cuba, for example, dissident or independent news sites that are perceived as critical—such as *Cubanet*, *Penúltimos Días*, *Diario de Cuba*, *Cubaencuentro*, *Hablemos Press*, and *14ymedio*—are restricted at most internet access points.

- **Corruption allegations** were subject to censorship in 28 out of 65 countries. Starting in July 2015, the Malaysian government, which had pledged never to censor the internet, blocked prominent blogs and news websites for the first time. The sites had reported on a billion-dollar corruption scandal implicating Prime Minister Najib Razak. The content-sharing platform Medium was blocked completely after one of the previously affected sites used it to repost content.

- News and opinion on **conflict**, terrorism, or outbreaks of violence were subject to censorship in 27 out of 65 countries. Sensitivity about ongoing conflict resulted in legitimate content being censored. In May 2016, British journalist Martyn Williams challenged South Korean regulators for blocking his website, North Korea Tech.

- **Social commentary** on issues including history and natural disasters was censored in 21 out of 65 countries. In August 2015, Ecuador prohibited independent reporting on the newly active volcano Cotopaxi. Citizens turned to social media for news, and as a result the government announced legal actions against users for "unscrupulous" comments on social networks. In China, discussion of the 1989 crackdown on prodemocracy protesters in Tiananmen Square is censored so comprehensively that internet users in mid-2015 reported being unable to make online financial transfers in denominations of 6 or 4, numbers which connote the crackdown's June 4 anniversary.

- Twenty out of 65 countries censored **blasphemy**, or content considered insulting to religion, suppressing legitimate commentary about religious and other issues. In 2016, internet service providers in India were ordered to block jihadology.net, an academic repository of primary sources about Islamist militancy. In Brazil, artist Ana Smiles was ordered to remove images of religious figurines dressed as superheroes or famous artists from social media.

- Information by or about particular **ethnic groups** was subject to censorship in 13 out of 65 countries. In Turkey, where fighting between security forces and the Kurdistan Workers' Party (PKK) has escalated, dozens of websites and Twitter accounts belonging to journalists reporting on the conflict have been censored.

Images draw greater scrutiny

Images, a vivid and immediate way of communicating information online, became a new priority for censors around the world in the past year. Several governments blocked platforms that allow users to exchange images easily in a bid to contain social and political protests. In Vietnam, Instagram was blocked along with Facebook during environmental protests in 2016, after both tools were used to organize and share images of fish killed en masse by industrial pollution.

World leaders proved particularly sensitive to altered images of themselves circulating on social media. In Egypt, a photo depicting President Abdel Fattah al-Sisi with Mickey Mouse ears resulted in a three-year prison term for the 22-year-old student who posted it on Facebook. Three people in Zimbabwe were arrested for photos of President Robert Mugabe that they shared in satirical social media posts.

Journalists were often targeted for disseminating images as part of their work. Police in Kenya arrested journalist Yassin Juma for using Facebook to report on and share photos of casualties in an attack on Kenyan forces stationed in Somalia. Egyptian photojournalist Ali Abdeen was arrested in April 2016 for covering protests against the transfer of Egyptian islands to Saudi Arabia. He was convicted in May of inciting illegal protests, publishing false news, and obstructing traffic, though his employers at the news website El-Fagr confirmed that he was working on assignment.

Security Measures Threaten Free Speech and Privacy

In both democratic and authoritarian countries, counterterrorism measures raised the likelihood of collateral damage to free speech, privacy rights, and business operations. Although in some cases the actions were meant to address legitimate security concerns, 14 of the 65 countries assessed in *Freedom on the Net* approved new national security laws

or policies that could have a disproportionately negative effect on free speech or privacy, with especially threatening consequences for government critics and journalists in countries that lack democratic checks and balances. Meanwhile, high-profile terrorist attacks in Europe and the United States led to increased pressure on technology companies to cooperate more closely with law enforcement regarding access to user data.

14 of the 65 countries approved national security laws or policies that could have a negative effect on free speech or privacy.

Broad antiterrorism laws lead to unjust penalties

In numerous authoritarian countries, officials enforced antiterrorism and national security laws in a manner that produced excessive or entirely inappropriate punishments for online activity. In the gravest cases, such laws were used to crack down on nonviolent activists, prominent journalists, and ordinary citizens who simply questioned government policies or religious doctrine.

In December 2015, a court in Russia handed down the first maximum sentence of five years in prison for extremism to blogger Vadim Tyumentsev, who was charged for posting videos that criticized pro-Kremlin separatists in eastern Ukraine and called for the expulsion of refugees coming to Russia from the Ukrainian regions of Donetsk and Luhansk. In July 2016, a new Russian law increased the maximum prison term for justifying or inciting terrorism to seven years. Penalties are even harsher in Pakistan, where antiterrorism courts sentenced two men in separate cases to 13 years in prison for promoting sectarian hatred on Facebook. A lawyer for one of the men said he had only "liked" the post in question, which was described as "against the belief of Sunni Muslims."

Ethiopian blogger Zelalem Workagenehu was found guilty of terrorism for facilitating a course on digital security.

Overly broad definitions of terrorism often resulted in spurious convictions. In Jordan, activist Ali Malkawi was arrested for criticizing the stance of Arab and Muslim leaders regarding the plight of Myanmar's persecuted Rohingya minority. He was sentenced to three months in jail under the antiterrorism law for "disturbing relations with a friendly state." Ethiopian blogger Zelalem Workagenehu was found guilty of terrorism and sentenced to over five years in prison in May for facilitating a course on digital security.

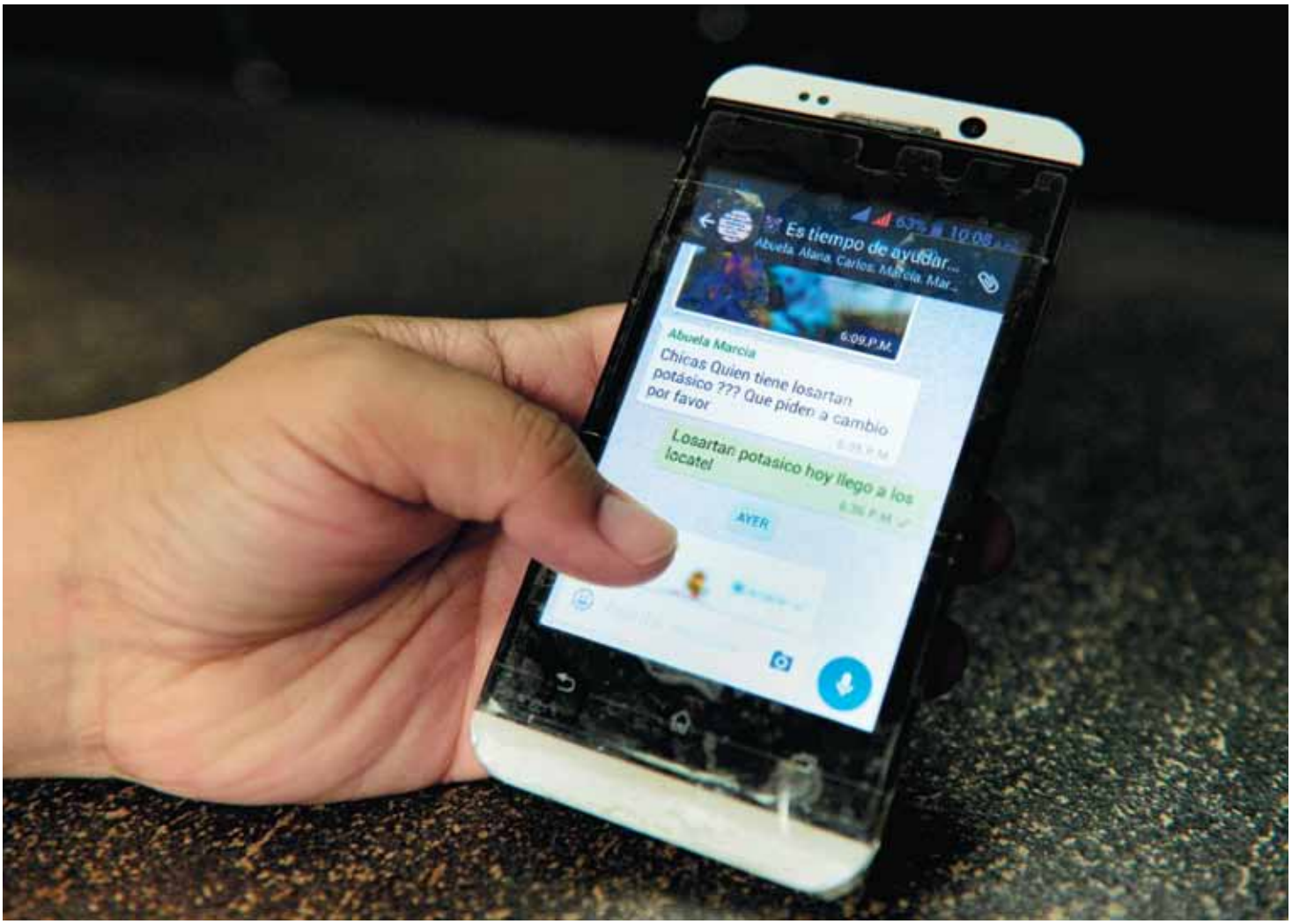
In some cases, journalists were branded as terrorists for independently documenting civil strife and armed conflicts. Sayed Ahmed al-Mousawi, an award-winning Bahraini photojournalist, was sentenced to 10 years in prison under an antiterrorism law in November 2015 due to his role in covering antigovernment protests and providing SIM cards to alleged "terrorists." Hayri Tunç, a Turkish journalist for the news site Jiyan, was sentenced to two years in prison for creating "terrorist propaganda" through his tweets, Facebook posts, and YouTube videos related to the conflict between the state and Kurdish militants.

Pressure to enable backdoor access

In democracies, where the definition of terrorism tends to have a narrower scope, debate has focused on the ability of intelligence and law enforcement agencies to prevent and prosecute terrorist attacks. As technology companies develop stronger privacy safeguards for their users, they have clashed with government entities attempting to gather information on suspected terrorists.

A United States district court ordered Apple to create new software that could bypass its own security measures and access a locked iPhone used by a perpetrator of the December 2015 terrorist attack in San Bernardino, California. Apple chief executive Tim Cook warned in a public letter that doing so would set a dangerous domestic legal precedent, embolden undemocratic governments to make similar requests, and make Apple products more vulnerable to hackers. U.S. authorities eventually dropped the case after experts were able to unlock the iPhone without Apple's help, leaving the broader legal issue unresolved.

Similarly, high-profile terrorist attacks in Europe have increased pressure to bolster the surveillance powers of government agencies tasked with disrupting future plots. France has extended a state of emergency since a major attack struck Paris in November 2015, autho-



Venezuelans rely on secure messaging tools to exchange information about scarce goods. Online content about currency exchange rates is pervasively censored.

rizing security agencies to monitor and detain individuals with little judicial oversight. Germany passed a law mandating the retention of telecommunications data by providers for up to 10 weeks, despite fierce protests from the opposition and a 2014 ruling by the EU's Court of Justice that such blanket requirements contravene fundamental rights. In August 2016, interior ministers from both countries called on the European Commission to draft an EU-level framework for compelling the makers of encrypted chat apps to hand over decrypted data in terrorism cases.

Authoritarian states have also joined the fray, but with far fewer scruples about individual rights. In Russia, for example, a draconian antiterrorism law passed in June 2016 requires all "organizers of information online"—which in theory could include local service providers as well as foreign social media companies—to provide the Federal Security Service (FSB) with tools to decrypt any information they transmit, essentially mandating backdoor access. The law will also require service providers to keep users' metadata for up to three years and the content of users' communications—calls, texts, images, videos, and other data—for up to six months.

Faced with growing pressure to comply with government requests, some tech companies have pushed back. Shortly after the Apple case, Microsoft sued the United States over the right to tell customers when data stored on the company's servers has been handed over to government agencies (Twitter initiated

Russia's new antiterrorism law requires all "organizers of information online" to provide the FSB with tools to decrypt any information they transmit.

a similar lawsuit in 2014). And in March 2016, roughly a billion people received a huge boost in their cybersecurity when Facebook rolled out end-to-end encryption for all WhatsApp users, incorporating technology from the makers of the security app Signal. However, such resistance is nearly impossible in countries that lack free and independent judicial institutions. Companies operating in authoritarian settings have little choice but to leave the market, comply with state demands, or risk blocking, closure, or imprisonment of their local staff.

Exploiting encryption's weakest links

Even when back doors are not installed, state entities and other actors have found ways to overcome cybersecurity and privacy safeguards. This year several governments exploited one of the weakest links in some encrypted apps: SMS authentication. Many platforms currently allow users to confirm their identity through a text message sent to their phone, whether to augment password security, replace forgotten passwords, or activate a new account. German agents reportedly intercepted these messages—which are unencrypted by default—in order to access the Telegram accounts of a neo-Nazi terrorist group suspected of plotting to attack a refugee shelter and assassinate Muslim clerics. The same technique was used in attempts to spy on nonviolent political and social activists in Egypt, Iran, and Russia over the past year. Companies and activists have recommended turning off SMS authentication in favor of code-generator apps.

In two-thirds of the countries under study, internet-based activism led to a tangible outcome.

Another potential weak link can be found in certificates, the small files that allow encrypted web traffic to travel to its destination and be decrypted for access by the intended recipient. Kazakhstan passed a new law requiring users and providers to install a "national security certificate" on all devices. While questions remain about how the requirement will be implemented in practice, observers worry that the measure will undermine cybersecurity for all Kazakh users by allowing security agencies or hackers to intercept and decrypt traffic before it reaches end users. If the law is successful, repressive countries around the world will look to Kazakhstan as a model for circumventing encryption in the name of national security.

New Heights in Digital Activism

As governments around the world impose new restrictions on internet freedom, it is worth remembering what is at stake. The present crackdown comes as digital platforms are being used in new and creative ways to advocate for change and, in many cases, save lives. Internet advocacy had real-world results in both democracies and authoritarian settings over the past year, and its impact was often most pronounced in countries where the information environment was more open online than off. In over two-thirds of the countries examined in this study, there was at least one significant example of individuals producing a tangible outcome by using online tools to fight for internet freedom, demand political accountability, advance women's rights, support victims of unjust prosecution, or provide relief to those affected by natural disasters.

Fighting for internet freedom and digital rights

Social media were used effectively to fight for internet freedom in a variety of countries over the past year. In Thailand, over 150,000 people signed a Change.org petition against a government plan to centralize the country's internet gateways, which would strengthen the authorities' ability to monitor and censor online activity. As a result, the government announced that it had scrapped the plan, though skeptical internet users remain vigilant.

Using the hashtag #NoToSocialMediaBill, Nigerian digital rights organizations launched a multifaceted campaign to defeat a "Frivolous Petitions Prohibition Bill" that threatened to constrain speech on social media. Alongside significant digital media activism, civil society groups organized a march on the National Assembly, gathered signatures for a petition presented during a public hearing on the bill, and filed a lawsuit at the Federal High Court in Lagos, all of which contributed to the bill's withdrawal in May 2016. India's telecommunications regulator banned differential pricing schemes in February after more than a million comments were submitted online to protest companies that charge consumers different prices for select content or applications.

Protesting governments and demanding accountability

Social media were also used to combat corruption, wasteful spending, or government abuse. Movements like Lebanon's #YouStink or #ElectricYerevan in Armenia channeled citizens' anger over bread-

KEY INTERNET CONTROLS BY COUNTRY

Freedom House documented how governments censor and control the digital sphere. Each colored cell represents at least one occurrence of the cited control during the report's coverage period of June 2015 to May 2016; colored cells with an asterisk (*) represent events that occurred between June and September 2016, when the report was sent to press. The Key Internet Controls reflect restrictions on content of political, social, or religious nature. For a full explanation of the methodology, see page 31.

Types of key internet controls

COUNTRY	# KICs employed	Social media or communications apps blocked	Political, social, or religious content blocked	Localized or nationwide ICT shutdown	Progovernment commentators manipualte online discussions	New law or directive increasing censorship or punishment passed	New law or directive increasing surveillance or restricting anonymity passed	Blogger or ICT user arrested, imprisoned, or in prolonged detention for political or social content	Blogger or ICT user physically attacked or killed (including in custody)	Technical attacks against government critics or human rights organizations	FOTN SCORE
Angola	2					*					40
Armenia	3	*									30
Azerbaijan	6										57
Bahrain	8			*							71
Bangladesh	5										56
Belarus	5										62
Brazil	2										32
Cambodia	4										52
Canada	1										16
China	9										88
Cuba	5										79
Ecuador	4										41
Egypt	7										63
Ethiopia	8					*	*				83
France	2										25
The Gambia	7	*									67
Georgia	1										25
Hungary	1						*				27
India	4										41
Indonesia	3										44
Iran	5										87
Jordan	5								*		51
Kazakhstan	9										63
Kenya	2										29
Kyrgyzstan	2										35
Lebanon	3										45
Libya	4										58
Malawi	1										41
Malaysia	4										45
Mexico	4										38
Morocco	4										44
Myanmar	3										61
Nigeria	2										34
Pakistan	7						*				69
Russia	7										65
Rwanda	2										51
Saudi Arabia	5										72
Singapore	1										41
South Korea	4										36
Sri Lanka	1										44
Sudan	4										64
Syria	6										87
Thailand	4										66
Tunisia	4										38
Turkey	6										61
Uganda	4										42
Ukraine	4								*		38
United Arab Emirates	5										68
Uzbekistan	7										79
Venezuela	6										60
Vietnam	8										76
Zambia	2			*							38
Zimbabwe	2	*						*			56
June 2015 – May 2016 coverage period		21	32	13	26	18	11	45	20	25	
June 2016 – September 2016		3	0	2	0	2	3	1	2	0	
Total June 2015 – September 2016		24	32	15	26	20	14	46	22	25	

NO KEY INTERNET CONTROLS OBSERVED

	FOTN Score
Argentina	27
Australia	21
Colombia	32
Estonia	6
Germany	19
Iceland	6
Italy	25
Japan	22
Phillipines	26
South Africa	25
United Kingdom	23
United States	18

and-butter issues—a garbage crisis and energy price hikes, respectively—into sustained protests that brought thousands of people to the streets and extracted responses from the government. Citizens in Kyrgyzstan criticized the parliament's plan to spend some US$40,000 on 120 new chairs to replace those purchased only five years earlier. The campaign, called #120Кресел (120Chairs), received extensive coverage on Twitter and through news outlets, and lawmakers subsequently abandoned the plan.

The Syrian American Medical Society used WhatsApp to guide a veterinarian who delivered twin babies by caesarean section.

Even in some of the world's most closed societies, individuals have used smartphones to record and publicize instances of abuse by state officials. After a video showing abuse at a military academy went viral in Myanmar, public outrage forced the military to launch a high-level investigation, an unprecedented gesture toward accountability from the country's most untouchable institution. In Saudi Arabia, the head of Riyadh's Committee for the Promotion of Virtue and the Prevention of Vice was dismissed in a bid to quell popular unease over a video in which members of the so-called morality police chased a girl outside a mall in the Saudi capital.

Defending women's rights around the globe

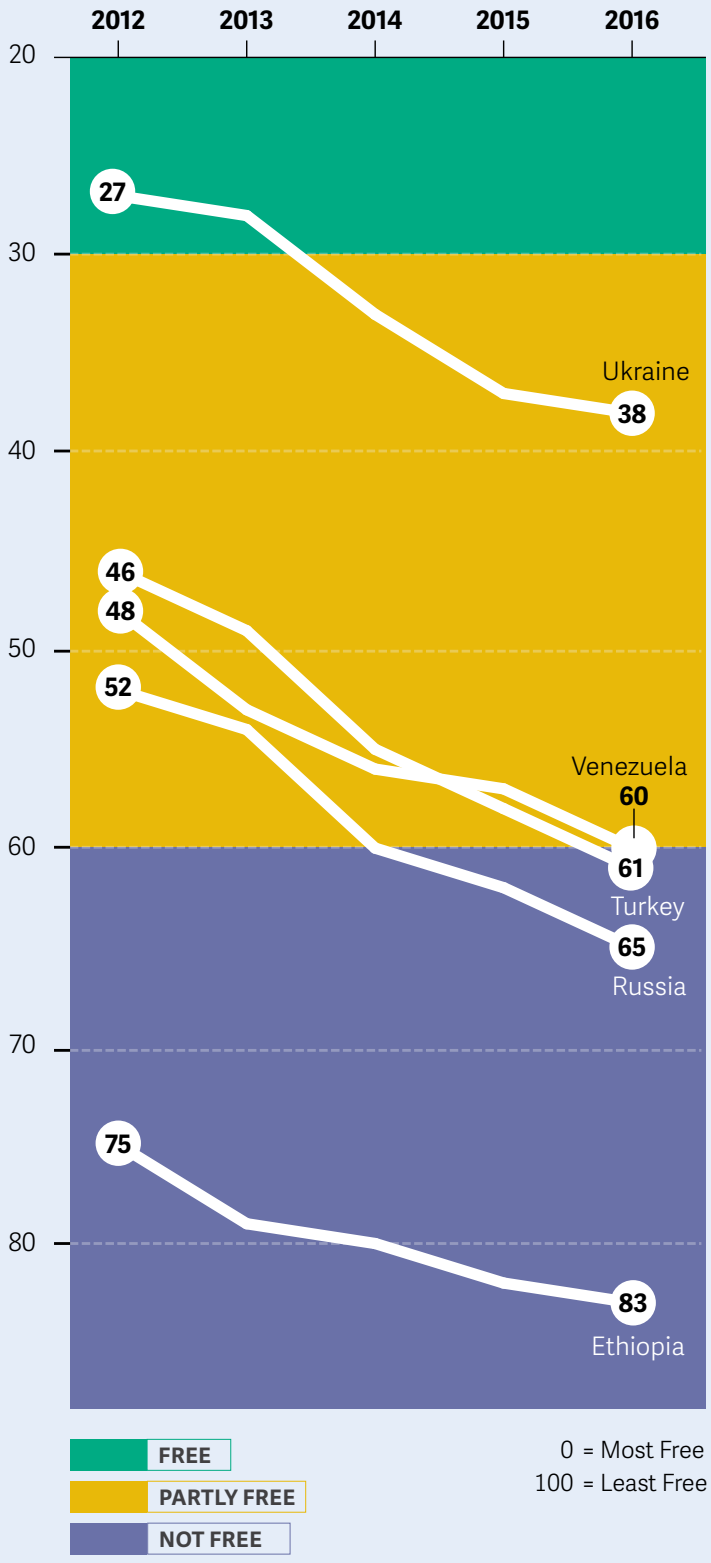
Several countries featured notable internet-based campaigning for women's rights. A Jordanian activist launched a popular online petition asking the parliament to amend Article 123 of the civil law, which requires that a male guardian be present for children to be admitted at hospitals. The National Council for Family Affairs, chaired by Queen Rania, later drafted legislation that created an exception in cases of emergency. In Argentina, the alarming rate of femicide and other gender-based violence led to an ongoing campaign, #NiUnaMenos (Not One Less), that has generated almost 300,000 tweets and inspired hundreds of thousands of people to demonstrate on June 3 of 2015 and 2016.

Disaster relief and saving lives during wartime

There were numerous instances during the year of social media and communication apps enabling crucial information-sharing that was credited with saving lives. Citizens and organizations have used digital tools to organize relief efforts, solicit donations, and disseminate information about rescue operations. In Sri Lanka, taxi apps like PickMe introduced an SOS button that allowed customers trapped in flood-affected areas to mark their location for rescue. And some of the most extraordinary uses of social media took place in Syria, where online applications have long been vital for citizen journalists and civic activists. The Syrian American Medical Society has used WhatsApp for telemedicine, in one instance guiding a veterinarian who delivered twin babies by caesarean section in the besieged town of Madaya.

Such examples of activism indicate that the internet is an indispensable tool for promoting social justice and political liberty, used by citizens worldwide to fight for their rights, demand accountability, and amplify marginalized voices. This is precisely why authoritarian governments are intensifying their efforts to impose control, and why democratic societies must simultaneously defend internet freedom abroad and uphold their own standards at home.

LARGEST FIVE-YEAR DECLINES



Of the 65 countries covered by *Freedom on the Net*, these five countries have experienced the steepest deterioration in internet freedom over the last five years:

Ukraine's decline reflects the country's struggle to regain stability since the 2014 toppling of the Yanukovych regime and ongoing conflict with Russian-backed separatists. Engaged in an information war with the Kremlin, authorities arrested social media users who stray from the government narrative, while cyberattacks originating in Russia have destabilized critical infrastructure around the country.

Venezuela's economic crisis impeded internet access and sharpened discontent with new president Nicolas Maduro. Seeking to prevent the country's vibrant digital sphere from contributing to social unrest, the regime blocks independent reporting and manipulates online discussions. Twitter users and citizen journalists are increasingly detained, and in some cases beaten by state security agents and progovernment thugs.

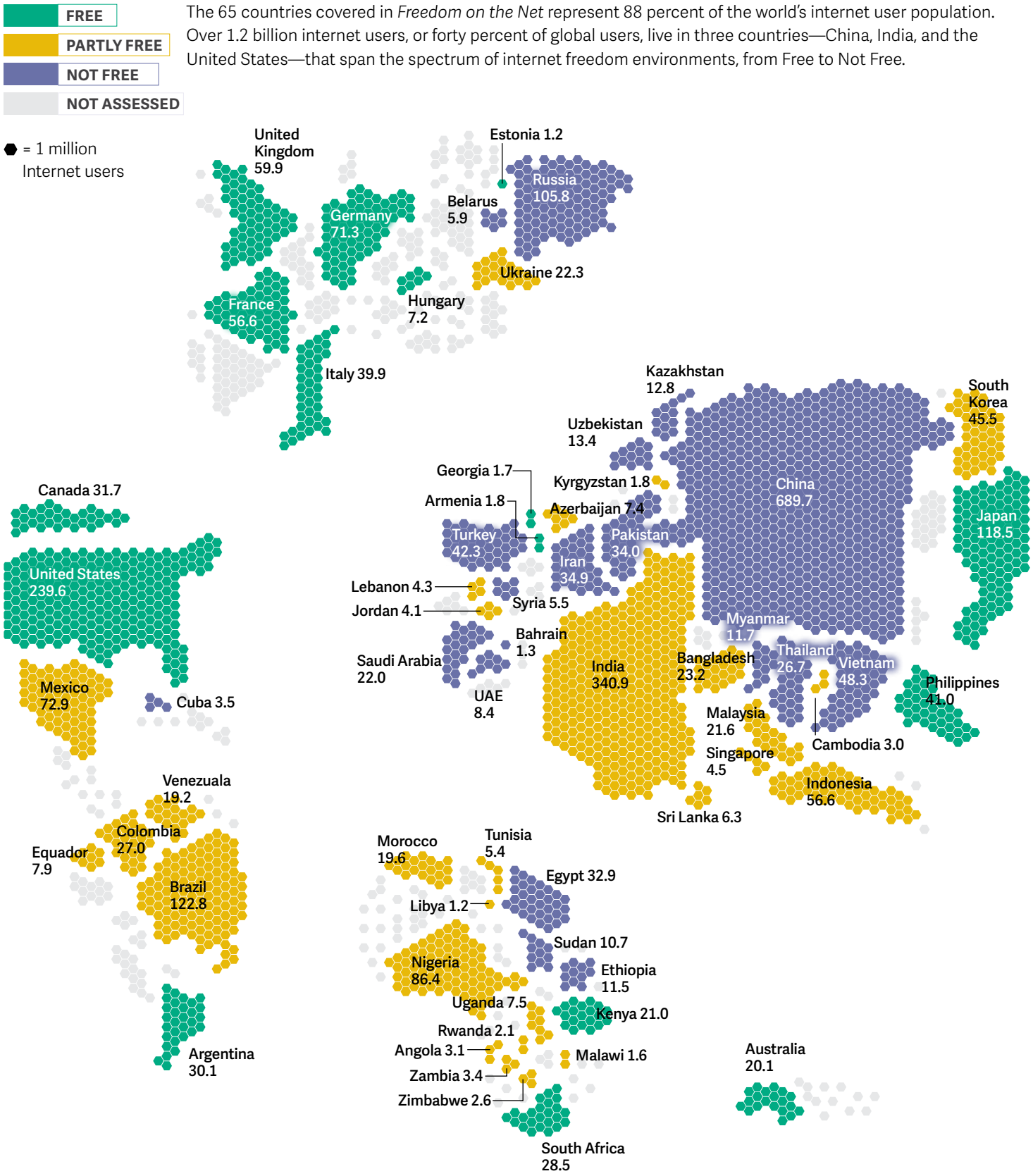
Internet freedom fell by 15 points in **Turkey**, the most drastic five-year decline recorded. President Erdogan oversaw a closing of the digital media sphere, often as a countermeasure to anti-government protests, corruption scandals, or terrorist attacks. Authorities are now more brazen to block social media platforms, demand companies remove "illegal" content, and prosecute individuals for "defaming" public figures.

The **Russian** government's tolerance for dissent diminished following the mass protests accompanying Vladimir Putin's election for a third presidential term in 2012. The regime consolidated power by promoting pro-Russia propaganda, upgrading surveillance technology, and censoring criticism of its Ukraine policy. In addition, new laws on blogger registration, data localization, and decryption requirements have undermined privacy.

Long one of the world's least connected countries, **Ethiopia** intensified its crackdown on bloggers and online journalists over the past five years. The regime has used terrorism laws to imprison individuals for simply calling attention to human rights issues. With ICT growth hindered by a state monopoly, the authorities maintain strict control over the digital sphere through a sophisticated filtering and surveillance apparatus.

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 1.2 billion internet users, or forty percent of global users, live in three countries—China, India, and the United States—that span the spectrum of internet freedom environments, from Free to Not Free.



GLOBAL INTERNET USER STATS

Over **3.2 billion people** have access to the internet.

According to Freedom House estimates:

67% live in countries where **criticism of the government, military, or ruling family** has been subject to censorship.

60% live in countries where ICT users were **arrested or imprisoned** for posting content on political, social, and religious issues.

49% live in countries where individuals have been **attacked or killed** for their online activities since June 2015.

47% live in countries where **insulting religion** online can result in censorship or jail time.

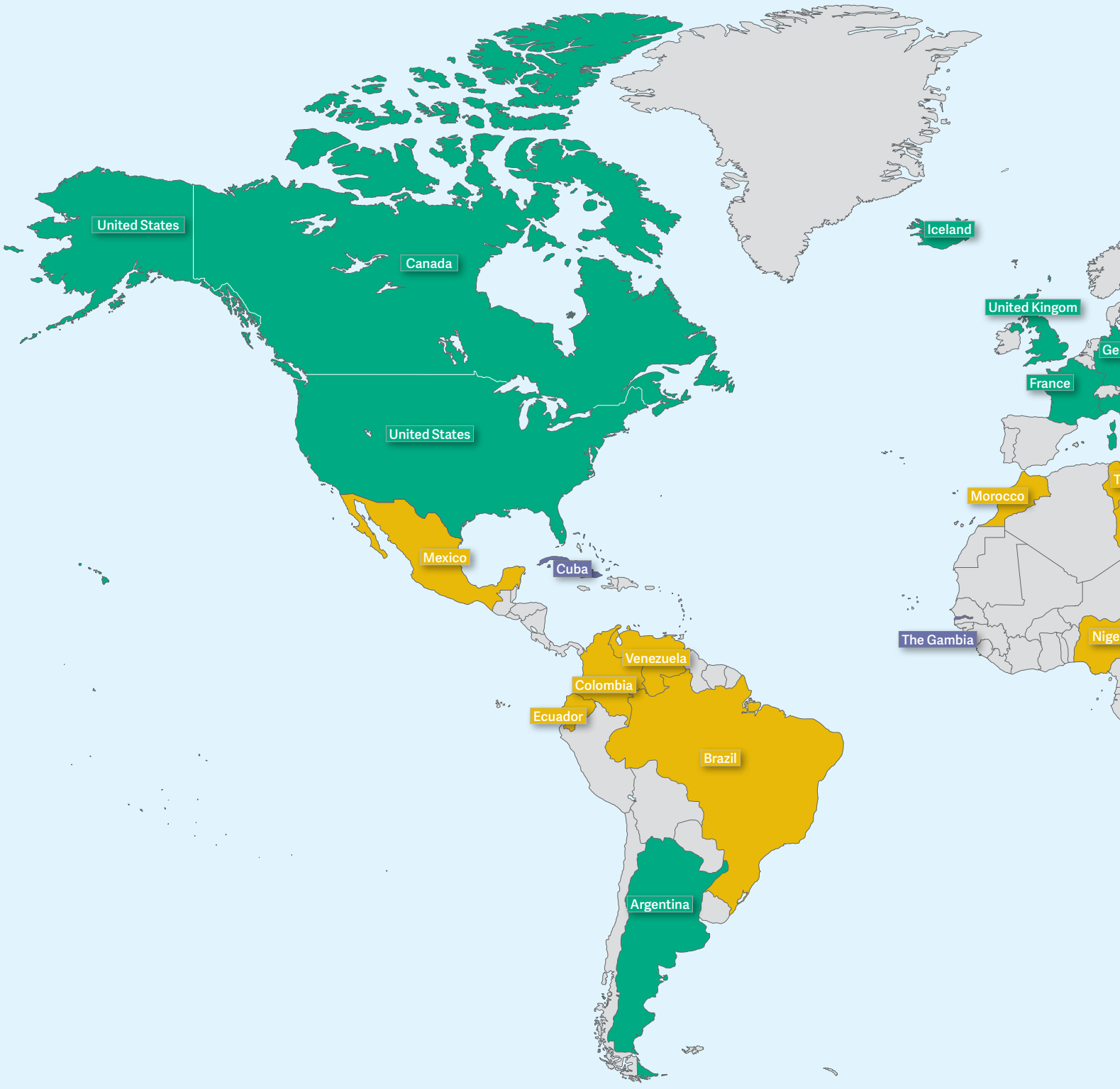
33% live in countries where online discussion of **LGBTI issues** can be repressed or punished.

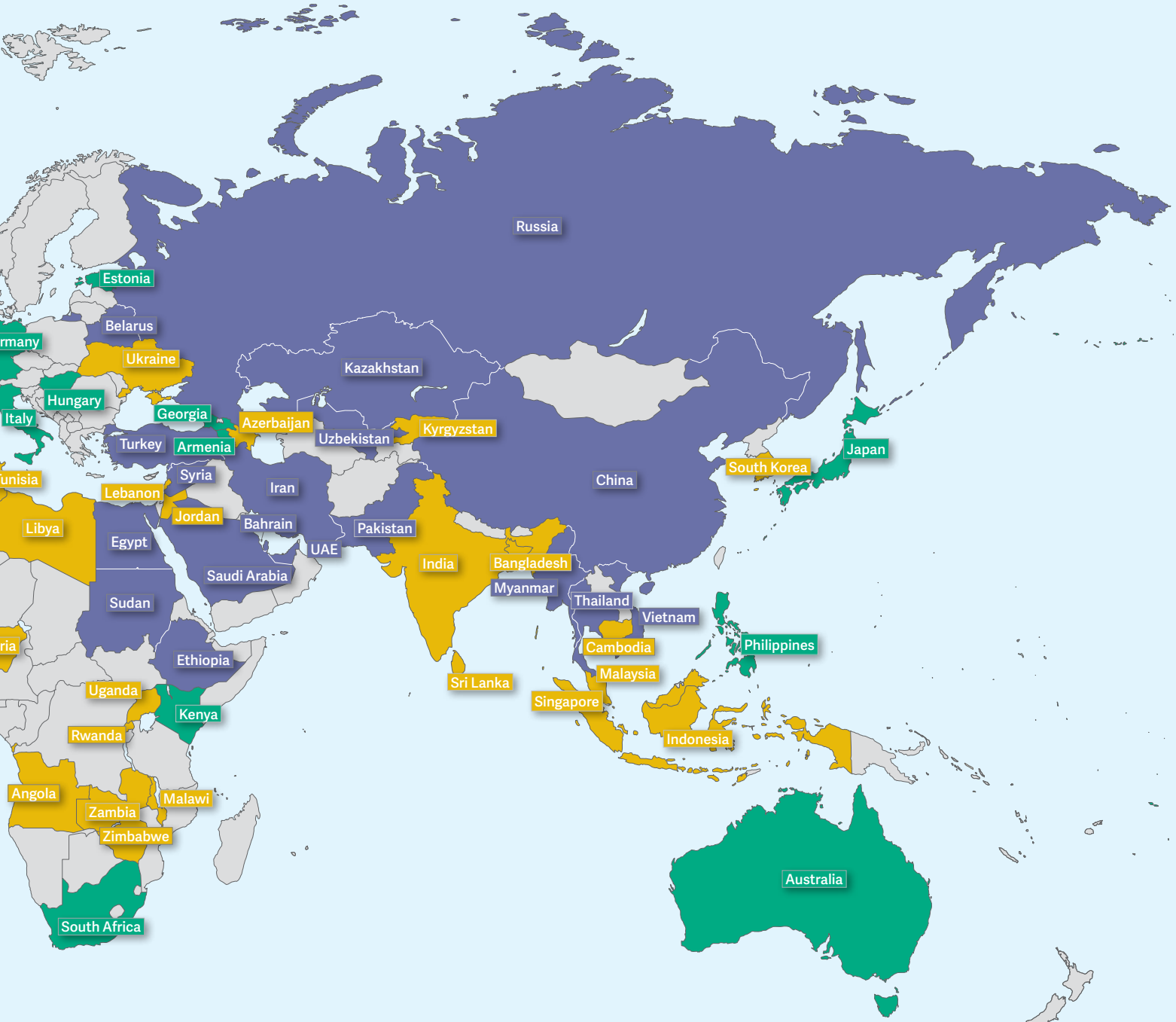
38% live in countries where **social media or messaging apps** were blocked over the past year.

27% live in countries where users have been arrested for **writing, sharing, or even liking Facebook posts**.

38% live under governments that **disconnected internet or mobile phone access**, often for political reasons.

FREEDOM ON THE NET 2016





Status	Countries
FREE	17
PARTLY FREE	28
NOT FREE	20
Total	**65**

Freedom on the Net 2016 assessed 65 countries around the globe. The project is expected to expand to more countries in the future.

65 COUNTRY SCORE COMPARISON

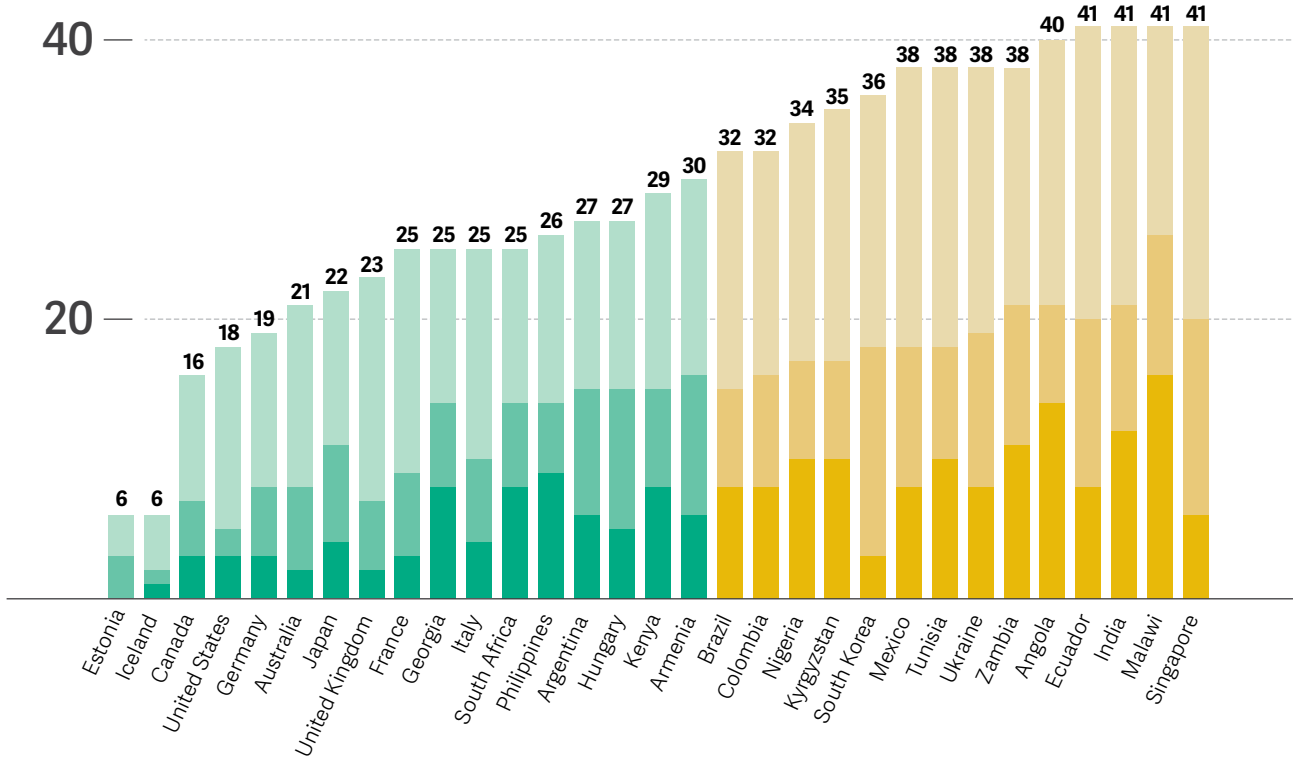
Freedom on the Net measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of FREE (0-30 points), PARTLY FREE (31-60 points),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

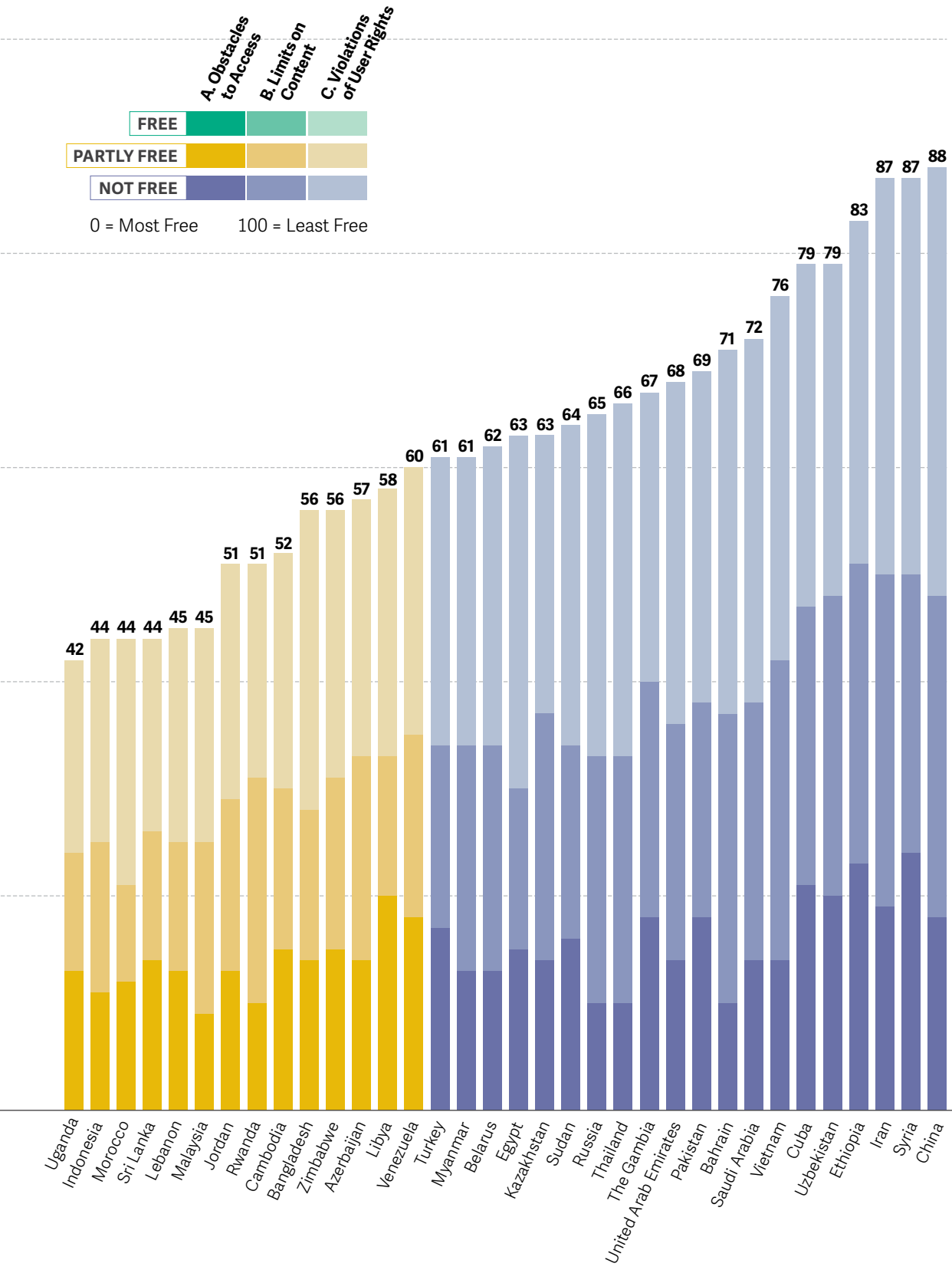
Ratings are determined through an examination of three broad categories:

A. OBSTACLES TO ACCESS: Assesses infrastructural and economic barriers to access; government 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.




A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights
FREE
PARTLY FREE
NOT FREE
0 = Most Free
100 = Least Free
42
44
44
44
45
45
51
51
52
56
56
57
58
60
61
61
62
63
63
64
65
66
67
68
69
71
72
76
79
79
83
87
87
88
Uganda
Indonesia
Morocco
Sri Lanka
Lebanon
Malaysia
Jordan
Rwanda
Cambodia
Bangladesh
Zimbabwe
Azerbaijan
Libya
Venezuela
Turkey
Myanmar
Belarus
Egypt
Kazakhstan
Sudan
Russia
Thailand
The Gambia
United Arab Emirates
Pakistan
Bahrain
Saudi Arabia
Vietnam
Cuba
Uzbekistan
Ethiopia
Iran
Syria
China

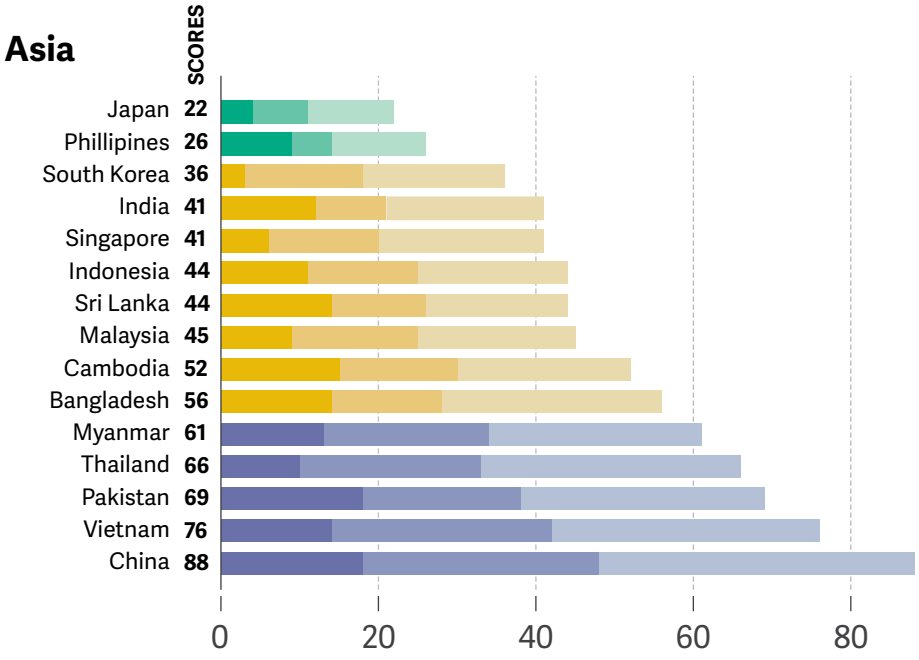
REGIONAL GRAPHS

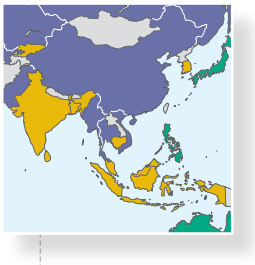
Freedom on the Net 2016 covers 65 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights

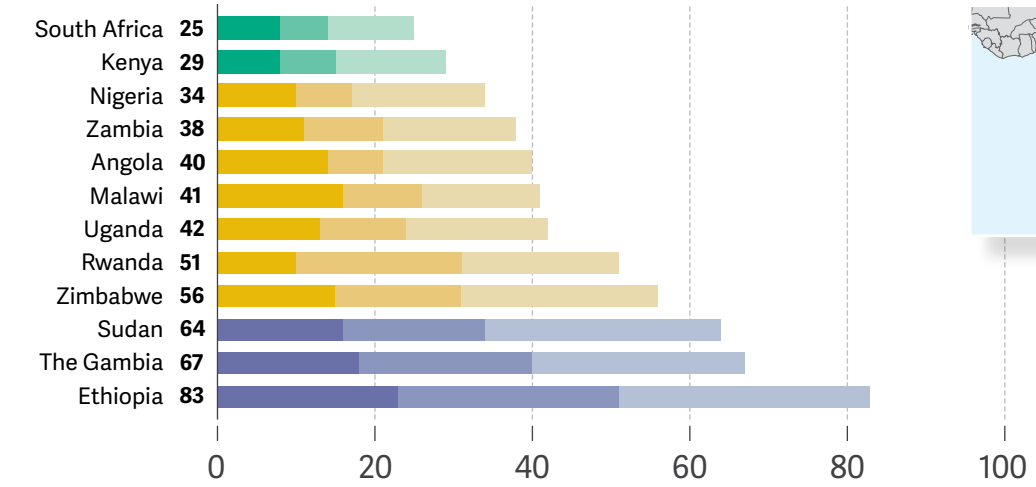
0 = Most Free
100 = Least Free

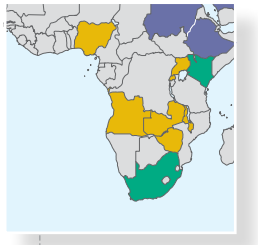
Asia



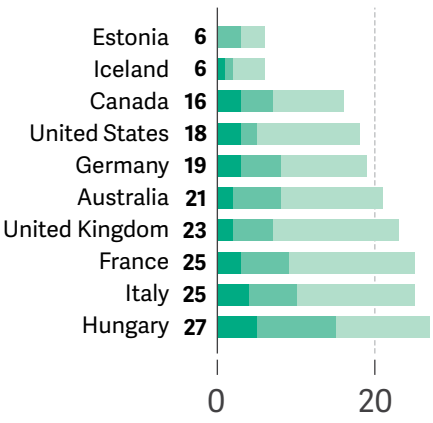


Sub-Saharan Africa

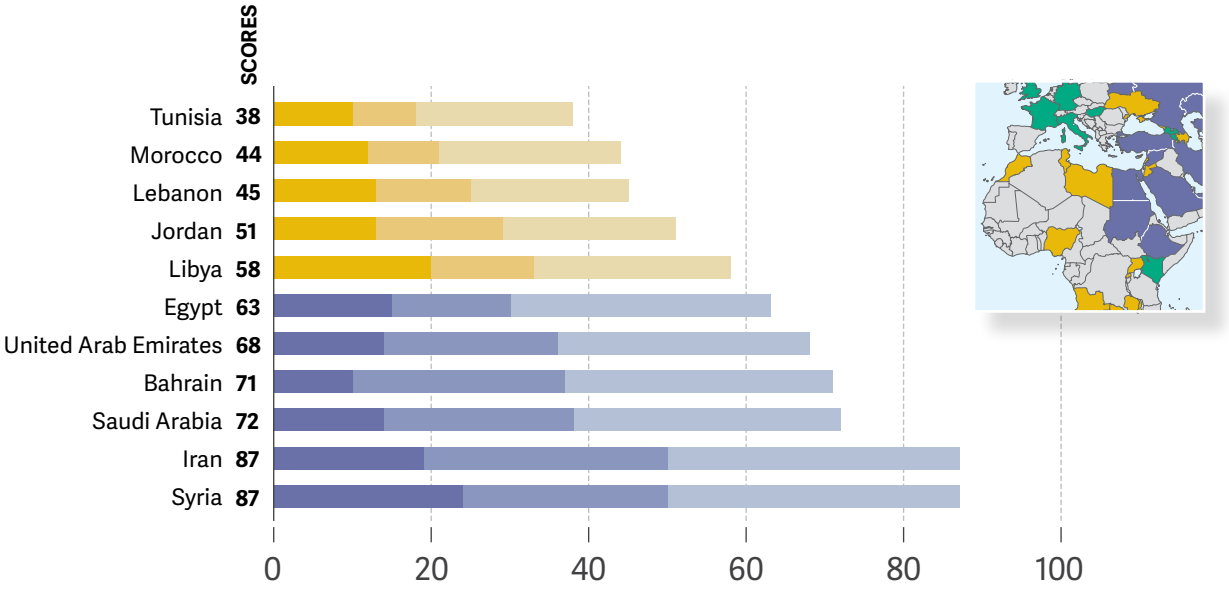




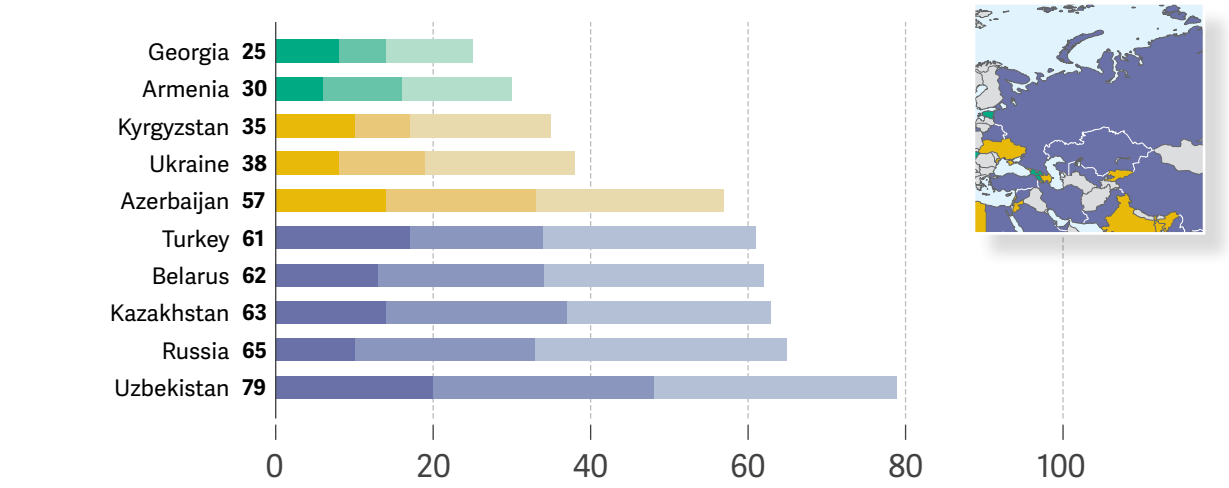
Australia, Canada, European Union, Iceland & United States



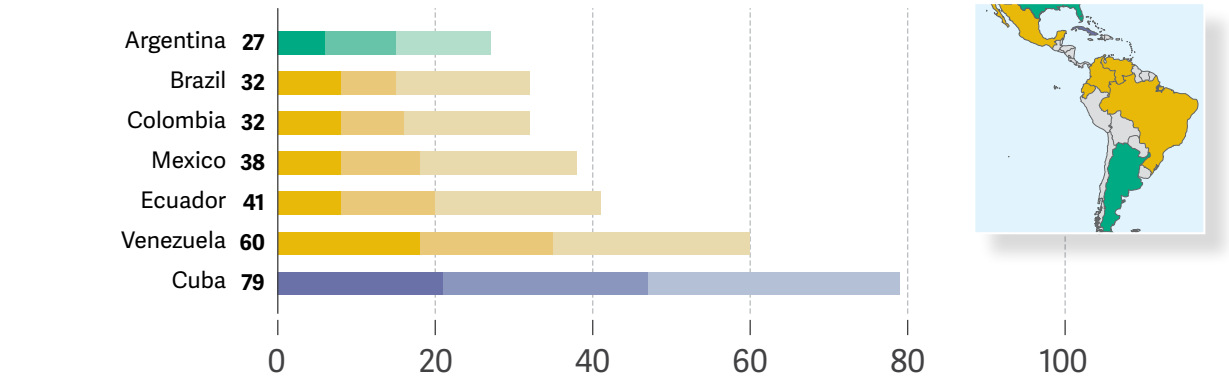
Middle East and North Africa (MENA)



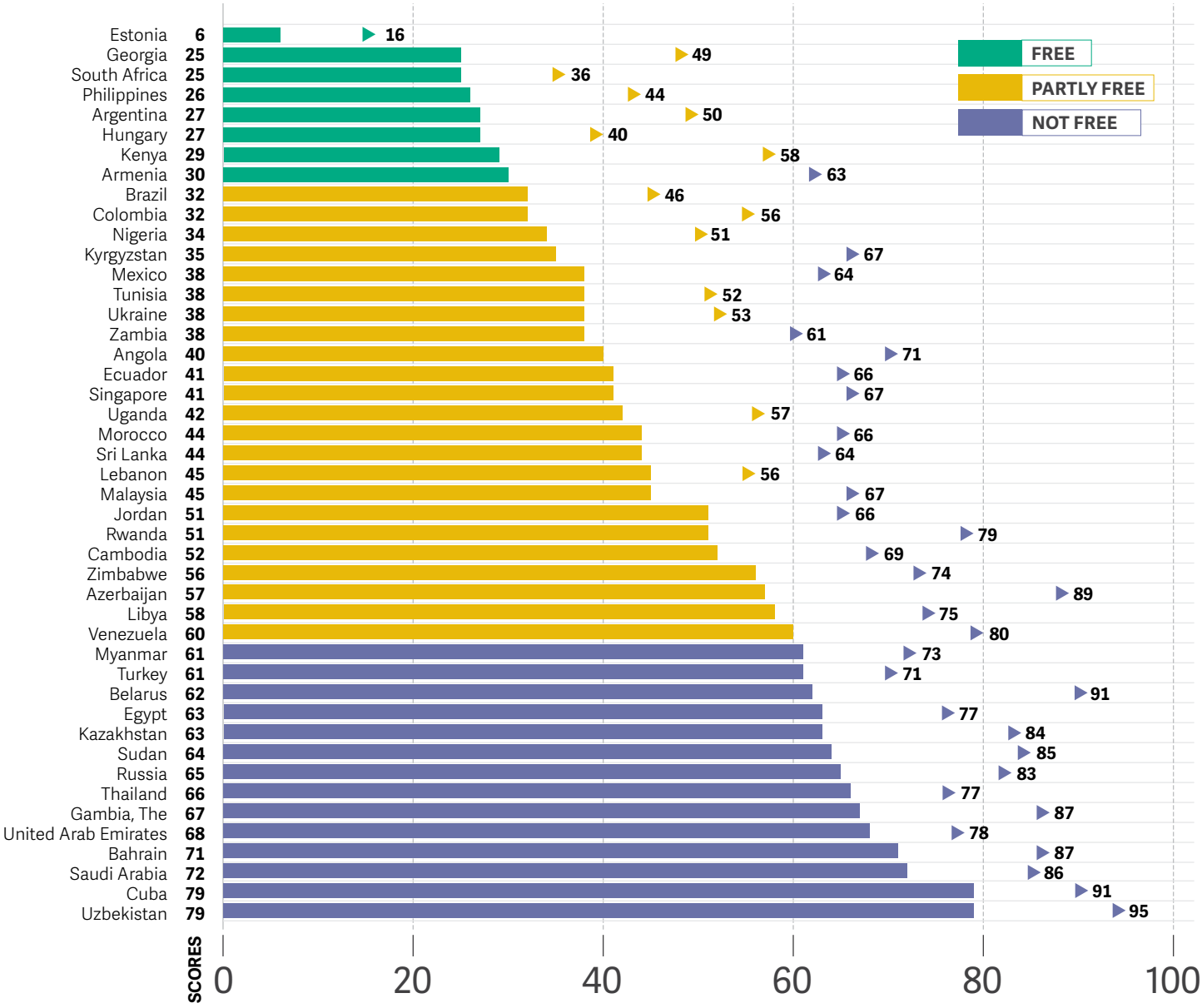
Eurasia



Latin America



INTERNET FREEDOM VS. PRESS FREEDOM

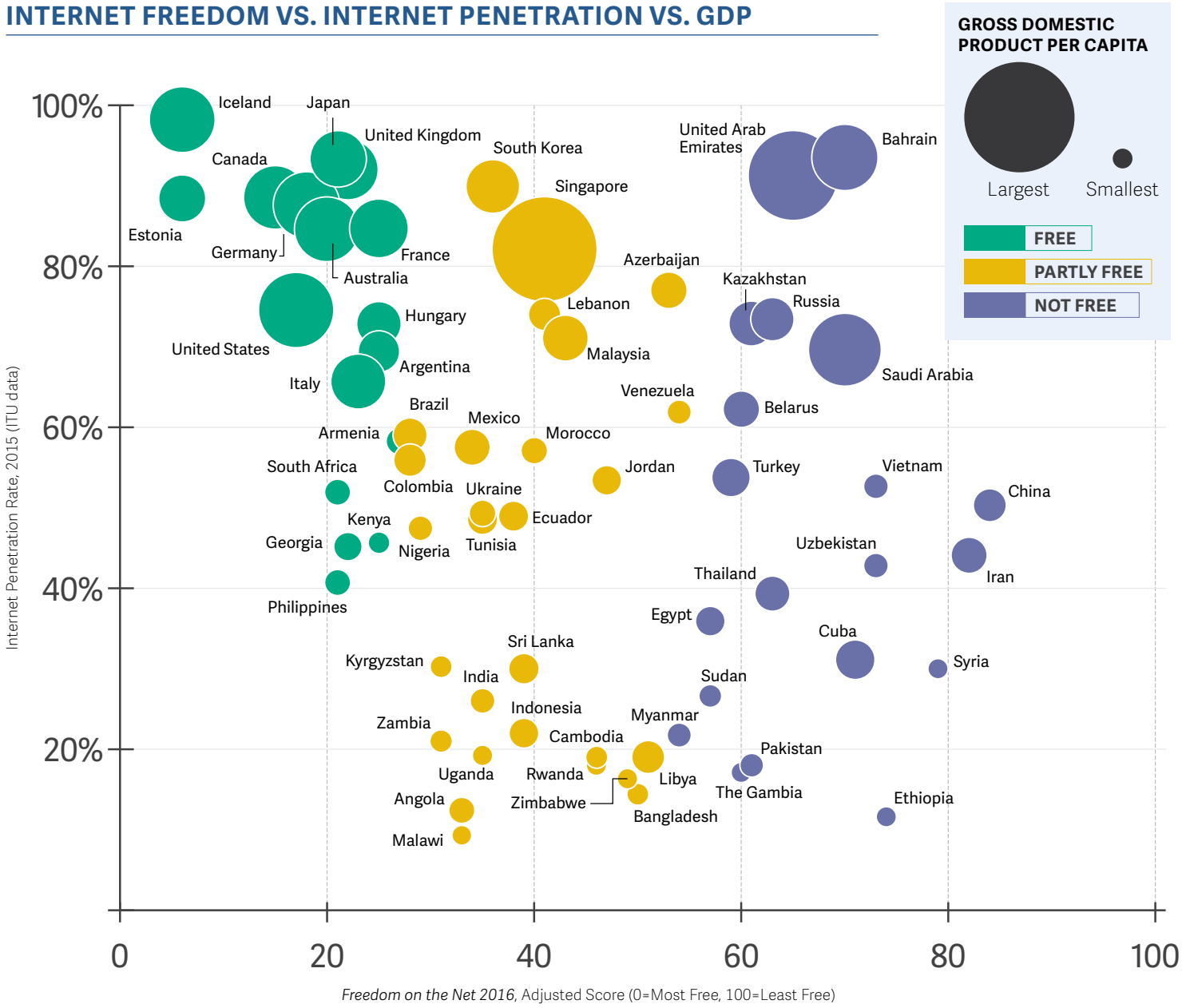


Freedom on the Net 2016 and *Freedom of the Press 2016* scores

In the majority of the 65 countries featured in this report, the internet is significantly more free than news media in general. This difference is evident from the comparison between a country's score on *Freedom on the Net 2016* (represented as the bar graph) and Freedom House's *Freedom of the Press 2016* assessment (represented as the scatterplot, ▶), the latter of which assesses a combination of broadcast, print, and online news media.

The figure above shows the 45 countries with a score difference of 10 points or higher, reflecting how the internet provides citizens with unprecedented access to information, even in the most repressive media environments. Nevertheless, *Freedom on the Net* research has consistently found that government intentions and efforts to control the internet are on the rise, particularly as citizen journalism and traditional media have become more dependent on social media and communications platforms.

INTERNET FREEDOM VS. INTERNET PENETRATION VS. GDP



The figure above depicts the relationship between internet freedom, internet access, and a country's gross domestic product (GDP) per capita. The x-axis considers a country's score in the 2016 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 2015 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 and International Monetary Fund.

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 Scores & Trajectories						Status
Country	FOTN 2015	FOTN 2016	Overall Trajectory	A. Obstacles to Access		B. Limits on Content		C. Violations of User Rights		*Freedom on the Net* 2016
Asia										
Bangladesh	51	56	▼	14	▼	14	▼	28	▼	●
Cambodia	48	52	▼	15	▼	15		22	▼	●
China	88	88		18		30		40		●
India	40	41	▼	12		9	▲	20	▼	●
Indonesia	42	44	▼	11		14	▼	19		●
Japan	22	22		4		7		11		●
Malaysia	43	45	▼	9	▼	16	▼	20	▲	●
Myanmar	63	61	▲	17	▲	17		27	▲	●
Pakistan	69	69		18	▲	20		31	▼	●
Philippines	27	26	▲	9	▲	5		12		●
Singapore	41	41		6		14		21		●
South Korea	34	36	▼	3		15	▼	18	▼	●
Sri Lanka	47	44	▲	14		12	▲	18	▲	●
Thailand	63	66	▼	10	▼	23	▼	33	▼	●
Vietnam	76	76		14	▼	28	▲	34		●
Eurasia										
Armenia	28	30	▼	6		10		14	▼	●
Azerbaijan	56	57	▼	14	▼	19		24		●
Belarus	64	62	▲	13	▲	21		28		●
Georgia	24	25	▼	8	▼	6		11		●
Kazakhstan	61	63	▼	14		23		26	▼	●
Kyrgyzstan	35	35		10	▲	7	▲	18	▼	●
Russia	62	65	▼	10		23		32	▼	●
Turkey	58	61	▼	13		21	▼	27	▼	●
Ukraine	37	38	▼	8		11	▼	19		●
Uzbekistan	78	79	▼	20	▼	28		31		●
Latin America										
Argentina	27	27		6	▲	9	▼	12		●
Brazil	29	32	▼	8	▼	7	▼	17	▼	●
Colombia	32	32		8		8		16		●
Cuba	81	79	▲	21	▲	26	▲	32		●
Ecuador	37	41	▼	8		12	▼	21	▼	●
Mexico	39	38	▲	8	▲	10		20		●
Venezuela	57	60	▼	18	▼	17	▲	25	▼	●

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.

Country	Overall			Category Scores & Trajectories						Status
	FOTN 2015	FOTN 2016	Overall Trajectory	A. Obstacles to Access		B. Limits on Content		C. Violations of User Rights		*Freedom on the Net* 2016
Middle East & North Africa										
Bahrain	72	71	▲	10	▲	27		34		●
Egypt	61	63	▼	15	▼	15	▼	33	▲	●
Iran	87	87		19	▲	31		37	▼	●
Jordan	50	51	▼	13	▼	16		22		●
Lebanon	45	45		13		12		20		●
Libya	54	58	▼	20		13	▼	25	▼	●
Morocco	43	44	▼	12	▼	9		23		●
Saudi Arabia	73	72	▲	14	▲	24		34		●
Syria	87	87		24		26		37		●
Tunisia	38	38		10		8		20		●
United Arab Emirates	68	68		14		22		32		●
Sub-Saharan Africa										
Angola	39	40	▼	14		7	▲	19	▼	●
Ethiopia	82	83	▼	23		28		32	▼	●
The Gambia	65	67	▼	18		22	▼	27	▼	●
Kenya	29	29		8	▲	7		14	▼	●
Malawi	40	41	▼	16	▼	10	▲	15	▼	●
Nigeria	33	34	▼	10		7	▲	17	▼	●
Rwanda	50	51	▼	10	▲	21	▼	20	▼	●
South Africa	27	25	▲	8		6	▲	11		●
Sudan	65	64	▲	16	▲	18	▲	30	▼	●
Uganda	36	42	▼	13	▼	11	▼	18		●
Zambia	40	38	▲	11		10	▲	17		●
Zimbabwe	56	56		15		16		25		●
Australia, Canada, European Union, Iceland & United States										
Australia	19	21	▼	2		6	▼	13	▼	●
Canada	16	16		3		4		9		●
Estonia	7	6	▲	0	▲	3		3		●
France	24	25	▼	3		6		16	▼	●
Germany	18	19	▼	3	▲	5		11	▼	●
Hungary	24	27	▼	5	▼	10	▼	12	▼	●
Iceland	6	6		1		1		4		●
Italy	23	25	▼	4		6		15	▼	●
United Kingdom	24	23	▲	2		5	▲	16		●
United States	19	18	▲	3		2		13	▲	●

▼ = Decline ▲ = Improvement
Blank = No Change

FREE | PARTLY FREE | NOT FREE

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 accompanying country reports provide narrative detail to support the scores.

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 numerical ratings and reports included in this study particularly focus on developments that took place between June 1, 2015 and May 31, 2016, although the analysis in the Key Internet Controls graph and the Topics Censored table covers developments through the end of September, when this year's edition was sent to press.

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 2016, 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 15), Freedom House documented how governments censor and control the digital sphere. Each colored cell represents at least one occurrence of the cited control during the report's coverage period of June 2015 to May 2016; colored cells with an asterisk (*) represent events that occurred from June until the time of writing (September 2016). Incidents are based on *Freedom on the Net* research and verified by in-country researchers. The Key Internet Controls reflect restrictions on content of political, social, or religious nature.

- **Social media or communications apps blocked:** Entire apps or key functions of social media, messaging, and calling platforms temporarily or permanently blocked to prevent communication and information sharing.
- **Political, social, or religious content blocked:** Blocking or filtering of domains, URLs, or keywords, to limit access to specific political, social, or religious content.
- **Localized or nationwide ICT shutdown:** Intentional disruption of internet or cellphone networks in

response to political or social events, whether temporary or long term, localized or nationwide.

- **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.
- **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.
- **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.
- **Blogger or ICT user arrested, imprisoned, or in prolonged detention for political or social content:** Any arrest, prosecution, detention that is credibly perceived to be in reprisal for digital expression, including trumped up charges. Brief detentions for interrogation are not reflected.
- **Blogger or ICT user physically attacked or killed (including in custody):** Any physical attack, kidnapping, or killing that is credibly perceived to be in reprisal for digital expression. This includes attacks while in custody, such as torture.
- **Technical attacks against government critics or human rights organizations:** Cyberattacks against human rights organizations, news websites, and 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 of attacks considered here may include critics in exile, but not transnational cyberattacks, even with political motives.

Censored Topics by Country Explained

In the Censored Topics by Country graphic (page 10), Freedom House staff documented a selection of topics that were subject to censorship in the 65 countries covered. Countries were included if state authorities blocked or ordered the removal of content, or detained or fined users for posting content on the topics considered. The chart does not consider extralegal pressures like violence, self-censorship, or cyberattacks, even where the state is believed to be responsible. To capture a comprehensive data set, the chart includes incidents over a two-year span, between June 2015 and September 2016, and distinguishes between pervasive and sporadic censorship. All data is based on *Freedom on the Net* research and verified by in-country researchers.

- **Criticism of the Authorities:** Content perceived as criticism of the state or its representatives, including the government, military, ruling family, police, judiciary, or other officials.
- **Political Opposition:** Content affiliated with political groups or opponents, including in the diaspora.
- **Corruption:** Accusations or exposés of corruption or misuse of public funds.
- **Blasphemy:** Content perceived as insulting or offending religion.
- **Mobilization for Public Causes:** Calls to protest or campaigns on political, social, or human rights issues.
- **Satire:** Humorous or ironic commentary on political or social issues.
- **Ethnic and Religious Minorities:** Content related to marginalized groups, including ethnic and religious minorities.
- **LGBTI Issues:** Content related to lesbian, gay, bisexual, transgender, or intersex individuals.
- **Conflict:** Discussion or reporting on local or international instances of violence, conflict, or terrorism.
- **Social Commentary:** Content that is not overtly political, including on economic, environmental, cultural, or educational issues.

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 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-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 informa-

tion 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 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, Director, *Freedom on the Net*
- Mai Truong, Program Manager (Africa)
- Adrian Shahbaz, Research Manager (MENA)
- Madeline Earp, Senior Research Analyst (Asia)
- Jessica White, Research Analyst (Latin America & EU)
- Rose Dlougatch, Senior Research Associate (Eurasia)

Report Authors and Advisors

- **Argentina:** Eduardo Ferreyra, Valeria Milanes, Jeannette Torrez, Leandro Ucciferri, Free Expression & Privacy team, Association for Civil Rights (ADC)
- **Armenia:** Artur Papyan, Internet Journalist at RFE/RL and media development consultant
- **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
- **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:** Allen Mendehlson, Canadian lawyer specializing in internet and technology law
- **Colombia:** Law, Internet, and Society Group, Fundación Karisma
- **Cuba:** Ernesto Hernández Busto, Cuban journalist and writer
- **Estonia:** Linnar Viik, Lecturer, Board Member, Estonian IT College
- **France:** Jean-Loup Richet, Researcher, University of Nantes
- **Georgia:** Teona Turashvili, E-Governance Direction Lead, 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:** Dalma Dojcsák and Máté Szabó, Hungarian Civil Liberties Union
- **Iceland:** Caroline Nellemann, independent consultant, specialist in digital media and civic engagement
- **India:** Sarvjeet Singh, Programme Manager, Centre for Communication Governance at National Law University, Delhi; Parul Sharma, Analyst, Center for Communication Governance; assistance from Nishtha Sinha and Vaibhav Dutt, Students, B.A., LL.B. (Hons.), National Law University
- **Indonesia:** Indriaswati Dyah Saptaningrum, Senior Researcher, ELSAM (The Institute for Policy Research and Advocacy)
- **Iran:** Kyle Bowen and Mahmood Enayat, Small Media
- **Italy:** Giampiero Giacomello, Associate Professor of International Relations, University of Bologna
- **Japan:** Dr. Leslie M. Tkach-Kawasaki, Associate Professor, University of Tsukuba

- **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, Program Manager, Public Policy Lab at the Issam Fares Institute for Public Policy and International Affairs, American University of Beirut
- **Libya:** Fadil Aliriza, journalist, researcher, political analyst, and Tunisia Project Manager, Carnegie Endowment for International Peace
- **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, Associate Professor of Media and Communication, Al Akhawayn University in Ifrane
- **Myanmar:** Min Zin, Executive Director, Institute for Strategy and Policy: Myanmar
- **Nigeria:** 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria
- **Pakistan:** Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan; Adnan Ahmad Chaudhri, Associate Researcher, Digital Rights Foundation
- **Russia:** Darya Luganskaya, freelance journalist
- **Singapore:** Cherian George, Associate Professor, School of Communication, Hong Kong Baptist University
- **South Africa:** Zororo Mavindidze, Senior Researcher, Freedom of Expression Institute
- **South Korea:** Dr. Yenn Lee, Doctoral Training Advisor, SOAS, University of London (School of Oriental and African Studies)
- **Sri Lanka:** N. V. Nugawela, consultant and researcher
- **Sudan:** Azaz Elshami, independent researcher and development consultant
- **Syria:** Dlshad Othman, information security expert
- **Uganda:** Lillian Nalwoga, Policy Officer, CIPESA, and President, Internet Society Uganda Chapter
- **Ukraine:** Tetyana Lokot, Ukrainian media researcher, Lecturer in Journalism, Dublin City University
- **United Kingdom:** Aaron Ceross, Researcher in Cyber Security, University of Oxford
- **United States:** Laura Reed, independent researcher
- **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), 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, Bangladesh, Belarus, China, Ecuador, Egypt, Ethiopia, The Gambia, Jordan, Rwanda, Philippines, Saudi Arabia, Thailand, Tunisia, Turkey, United Arab Emirates, Vietnam and Zimbabwe are independent internet researchers who have asked to remain anonymous.

Notes

“The internet is an indispensable tool for promoting social justice and political liberty, used by citizens worldwide to fight for their rights, demand accountability, and amplify marginalized voices.”

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