The Rise of Digital Authoritarianism

October 2018

Freedom House

FREEDOM ON THE NET 2018

Freedom on the Net 2018

Table of Contents

The Rise of Digital Authoritarianism **1**

Major Developments 6

Tables, Charts, and Graphs

FOTN 2018 Improvements and Declines 3

Global Internet Population by 2018 FOTN Status 5

The World Is Buying What China Is Selling 9

FOTN World Map 16

Key Internet Controls by Country 22

Largest Five-Year Declines 23

Global Rankings 24

Regional Rankings 26

Distribution of Global Internet Users by Country and FOTN Status 28

Recommendations **20**

This report was made possible by the generous support of the U.S. State Department's Bureau of Democracy, Human Rights and Labor (DRL), Dutch Ministry of Foreign Affairs, New York Community Trust, Google, Internet Society, and Oath.

The following people were instrumental in the research and writing of this report: Mai Truong, Jessica White, and Allie Funk. Tyler Roylance edited the report. Cheryl Yu and Andrew Greco provided research assistance.

This booklet is a summary of findings for the 2018 edition of *Freedom on the Net*. Narrative reports of the 65 countries assessed in this year's study and a full list of contributors can be found on our website at **www.freedomonthenet.org.**

ON THE COVER

A display shows a facial recognition system during the 1st Digital China Summit on April 22, 2018 in Fuzhou, China.

Photo credit: VCG/VCG via Getty Images

Freedom House

The Rise of Digital Authoritarianism

by Adrian Shahbaz

The internet is growing less free around the world, and democracy itself is withering under its influence.

Disinformation and propaganda disseminated online have poisoned the public sphere. The unbridled collection of personal data has broken down traditional notions of privacy. And a cohort of countries is moving toward digital authoritarianism by embracing the Chinese model of extensive censorship and automated surveillance systems. As a result of these trends, global internet freedom declined for the eighth consecutive year in 2018.

Events this year have confirmed that the internet can be used to disrupt democracies as surely as it can destabilize dictatorships. In April 2018, Facebook founder and chief executive Mark Zuckerberg testified in two congressional hearings about his company's role in the Cambridge Analytica scandal, in which it was revealed that Facebook had exposed the data of up to 87 million users to political exploitation. The case was a reminder of how personal information is increasingly being employed to influence electoral outcomes. Russian hackers targeted US voter rolls in several states as part of the Kremlin's broader efforts to undermine the integrity of the 2016 elections, and since then, security researchers have discovered further breaches of data affecting 198 million American, 93 million Mexican, 55 million Filipino, and 50 million Turkish voters.

With or without malign intent, the internet and social media in particular can push citizens into polarized echo chambers and pull at the social fabric of a country, fueling hostility between different communities. Over the past 12 months in Bangladesh, India, Sri Lanka, and Myanmar, false rumors and hateful propaganda that were spread online incited jarring outbreaks of violence against ethnic and religious minorities. Such rifts often serve the interests of antidemocratic forces in society, the government, or hostile foreign states, which have actively encouraged them through content manipulation.

China was once again the worst abuser of internet freedom in 2018.

As democratic societies struggle with the challenges of a more dangerous and contested online sphere, leaders in Beijing have stepped up efforts to use digital media to increase their own power, both at home and abroad. China was once again the worst abuser of internet freedom in 2018, and over the past year, its government hosted media officials from dozens of countries for two- and three-week seminars on its sprawling system of censorship and surveillance. Moreover, its compa-

Rising Digital Authoritarianism, by the Numbers

8 Consecutive years of global internet freedom declines

36 Countries with representatives who attended Chinese trainings and seminars on new media or information management

17 Governments approved or proposed laws restricting online media in the name of fighting "fake news" and online manipulation

18 Countries increased surveillance, often eschewing independent oversight and weakening encryption to gain unfettered access to data

nies have supplied telecommunications hardware, advanced facial-recognition technology, and data-analytics tools to a variety of governments with poor human rights records, which could benefit Chinese intelligence services as well as repressive local authorities. Digital authoritarianism is being promoted as a way for governments to control their citizens through technology, inverting the concept of the internet as an engine of human liberation.

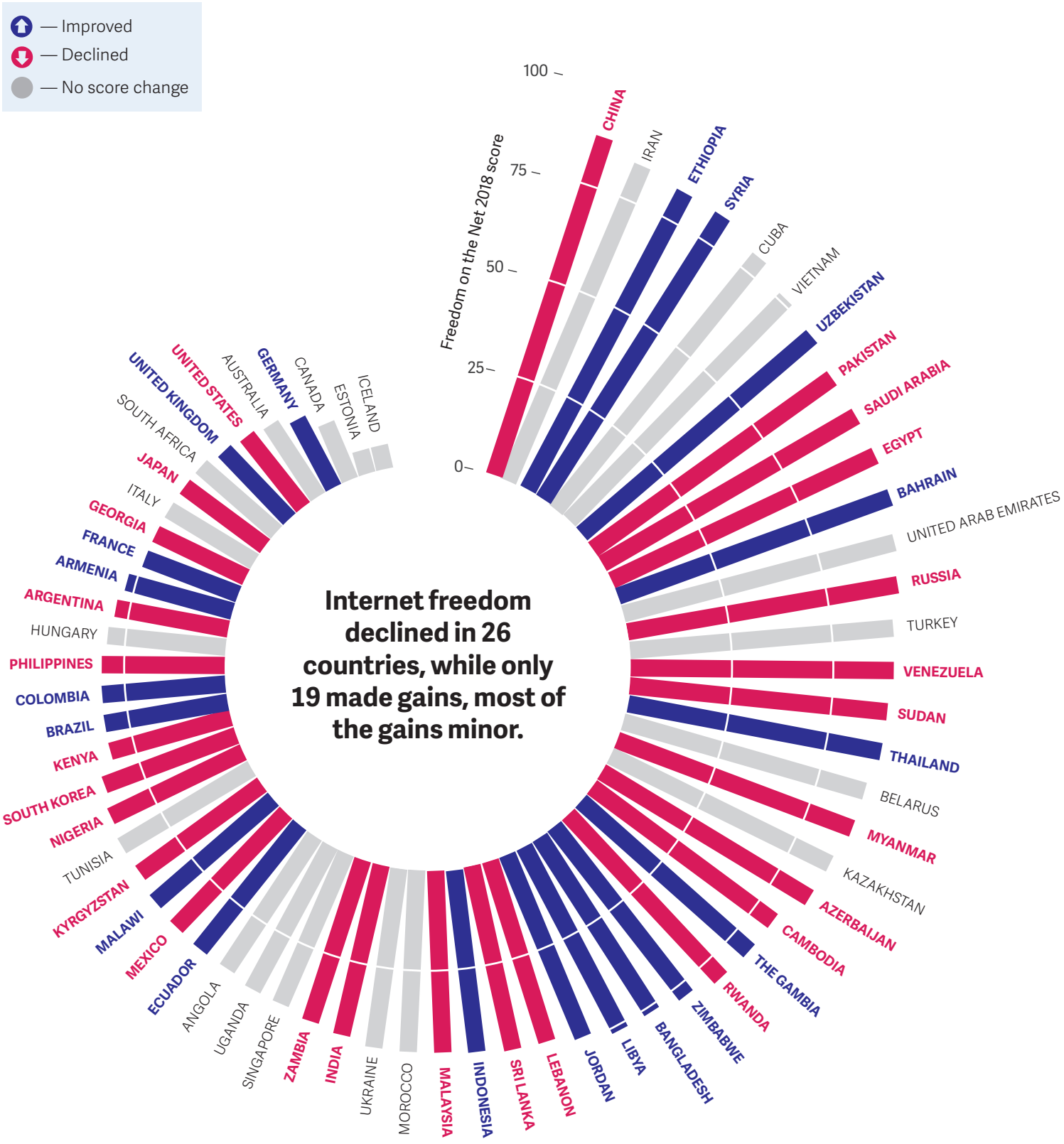
Throughout the year, authoritarians used claims of "fake news" and data scandals as a pretext to move closer to the China model. Governments in countries such as Egypt and Iran rewrote restrictive media laws to apply to social media users, jailed critics under measures designed to curb false news, and blocked foreign social media and communication services. China, Russia, and other repressive states are also demanding that companies store their citizens' data within their borders, where the information can be accessed by security agencies.

Democracies are famously slow at responding to crises—their systems of checks and balances, open deliberation, and public participation are not conducive to rapid decision-making. But this built-in caution has helped some semidemocratic countries fend off authoritarian-style internet controls over the past year. In May, Kenyan bloggers challenged the constitutionality of criminal provisions against the spread of false news, winning a suspension of the rules pending a final court judgment. That same month, Malaysians voted in a prime minister who promised to rescind a recently adopted law against fake news that was used by his predecessor in a failed attempt to sway the elections. Some countries are not just resisting setbacks, but making real progress on internet freedom. In a significant if imperfect step forward for user privacy, over 500 million citizens in the European Union gained new rights over their personal data on May 25 as part of the General Data Protection Regulation.

Securing internet freedom against the rise of digital authoritarianism is fundamental to protecting democracy as a whole. Technology should empower citizens to make their own social, economic, and political choices without coercion or hidden manipulation. The internet has become the modern public sphere, and social media and search engines have both tremendous power and a weighty responsibility to ensure that their platforms serve the public good. If antidemocratic entities effectively capture the internet, citizens will be denied a forum to articulate shared values, debate policy questions, and peacefully settle intrasocietal disputes. Democracy also requires a protected private sphere. The unrestrained and largely unexamined collection of personal data inhibits one's right to be let alone, without which peace, prosperity, and individual freedom—the fruits of democratic governance—cannot be sustained or enjoyed.

If democracy is to survive the digital age, technology companies, governments, and civil society must work together to find real solutions to the problems of social media manipulation and abusive data collection. Multilateral and cross-sectoral coordination is required to promote digital literacy, identify malicious actors, and deny them the tools to fraudulently amplify their voices. When it comes to protecting data, users must be granted the power to ward off undue intrusions into their personal lives by both the government and corporations. Global internet freedom can and should be the antidote to digital authoritarianism. The health of the world's democracies depends on it.

2018 FREEDOM ON THE NET IMPROVEMENTS AND DECLINES



Tracking the Global Decline

Freedom on the Net is a comprehensive study of internet freedom in 65 countries around the globe, covering 87 percent of the world's internet users. It tracks improvements and declines in internet freedom conditions each year. The countries included in the study are selected to represent diverse geographical regions and regime types. In-depth reports on each country can be found at www.freedomonthenet.org.

More than 70 analysts contributed to this year's edition using a 21-question research methodology that addresses internet access, freedom of expression, and privacy issues. In addition to ranking countries by their internet freedom score, the project offers a unique opportunity to identify global trends related to the impact of information and communication technologies on democracy. This report, the eighth in its series, focuses on developments that occurred between June 2017 and May 2018.

Of the 65 countries assessed, 26 have been on an overall decline since June 2017, compared with 19 that registered net improvements. The biggest score declines took place in Egypt and Sri Lanka, followed by Cambodia, Kenya, Nigeria, the Philippines, and Venezuela.

Even as the #MeToo movement successfully exposed rampant sexual assault and harassment in some parts of the world, two women in Egypt were arrested in separate incidents for uploading video confessionals on Facebook to decry such abuses in that country. Both were accused of spreading false information to harm public security; one, a visiting Lebanese tourist, was sentenced to eight years in prison. Egyptian authorities undertook a broader crackdown on dissent by blocking some 500 websites, including those of prominent human rights organizations and independent media outlets. In Sri Lanka, authorities shut down social media platforms for two days during communal riots that broke out in March and led to at least two deaths. Rumors and disinformation had spread on digital platforms, sparking vigilante violence that predominantly targeted the Muslim minority.

In almost half of the countries where internet freedom declined, the reductions were related to elections. Twelve countries suffered from a rise in disinformation, censorship, technical attacks, or arrests of government critics in the lead-up to elections. As Venezuela held a presidential election in May to cement the authoritarian rule of Nicolás Maduro, the government passed a vaguely written law that imposed severe prison sentences for inciting "hatred" online. Implementation of the "Fatherland Card"—an electronic identification system used to channel social aid—stirred suspicions that data collected through the device could be exploited to monitor and pressure voters. Ahead of general elections in July 2018, Cambodia experienced a surge in arrests and prison sentences for online speech, as the government sought to broaden the arsenal of offenses used to silence dissent, including a new lèse-majesté law that bans insults to the monarchy.

Score declines in the Philippines and Kenya led to status downgrades. The Philippines slipped from Free to Partly Free as content manipulation and cyberattacks threatened to distort online information. Harassment of dissenting voices escalated, with authorities attempting to close down a local news website known for its critical coverage of President Rodrigo Duterte's brutal war on drugs. The media organization Vera Files, one of several outlets to suffer cyberattacks during the year, was hit with a distributed denial-of-service (DDoS) attack shortly after it published a sensitive story about Duterte and his daughter's declaration of assets. In Kenya, which also moved from Free to Partly Free, online manipulation and disinformation targeted voters during the August 2017 elections, while a Cybercrime Law passed in May 2018 increased the maximum penalty for publishing "false" or "fictitious" information to 10 years in prison if the action results in "panic" or is "likely to discredit the reputation of a person," despite the fact that criminal defamation was ruled unconstitutional in 2017. An association of bloggers appealed provisions of the law, which were suspended for further review. These negative developments occurred against the backdrop

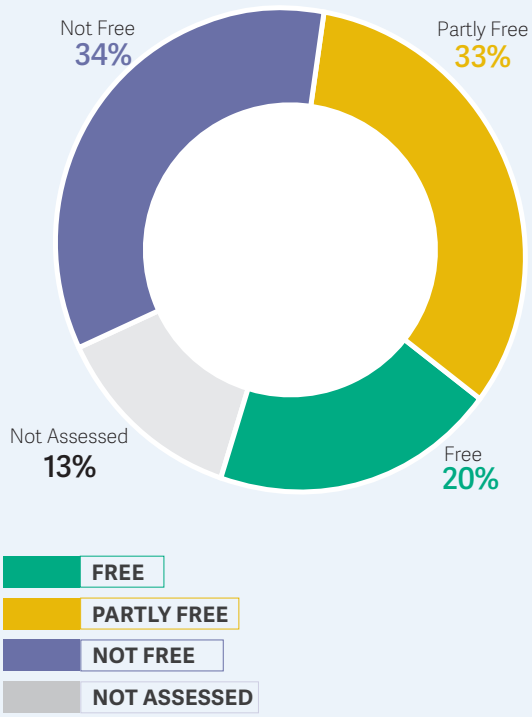
of growing surveillance concerns and ongoing arrests of bloggers and ordinary social media users for criticizing government officials or posting alleged hate speech.

Internet freedom declined in the United States. The Federal Communications Commission repealed rules that guaranteed net neutrality, the principle that service providers should not prioritize internet traffic based on its type, source, or destination. The move sparked efforts by civil society groups and state-level authorities to restore the protections on a local basis. In a blow to civil rights and privacy advocates, Congress reauthorized the FISA Amendments Act, including the controversial Section 702, thereby missing an opportunity to reform surveillance powers that allow the government to conduct broad sweeps in search of non-US targets and routinely collect the personal communications of Americans in the process. Despite an online environment that remains vibrant, diverse, and free, disinformation and hyperpartisan content continued to be of pressing concern in the United States, particularly in the run-up to the 2018 midterm elections.

Of the 19 countries with overall score improvements, two—Armenia and the Gambia—earned upgrades in their internet freedom status. Armenia rose from Partly Free to Free after citizens successfully used social media platforms, communication apps, and live-streaming services to bring about political change in the country's Velvet Revolution in April. The Gambia jumped from Not Free to Partly Free, as restrictions have eased and users have posted content more freely since longtime dictator Yahya Jammeh was forced from office in early 2017. However, many draconian laws enacted under the former regime are still in place. While Ethiopia remained highly repressive, a new prime minister appointed in April 2018 immediately moved to reduce tight internet restrictions and promised broader reforms. Prominent bloggers were released from prison, and citizens felt more free to speak out on social media and participate in their country's potential transition from authoritarian rule.

GLOBAL INTERNET POPULATION BY 2018 FOTN STATUS

FOTN assesses 87 percent of the world's internet user population.



Of the 65 countries assessed, 26 have been on an overall decline since June 2017, compared with 19 that registered net improvements.

Major Developments

China remakes the world in its techno-dystopian image

US president Bill Clinton famously compared the Chinese government's attempts to control the internet to "trying to nail Jell-O to the wall." But over the last two decades, the country's "Great Firewall" has grown into an alarmingly effective apparatus of censorship and surveillance. This year, Beijing took steps to propagate its model abroad by conducting large-scale trainings of foreign officials, providing technology to authoritarian governments, and demanding that international companies abide by its content regulations even when operating outside of China. These trends present an existential threat to the future of the open internet and prospects for greater democracy around the globe.

Internet controls within China reached new extremes in 2018 with the implementation of the sweeping Cybersecurity Law and upgrades to surveillance technology.

The China model at home

Internet controls within China reached new extremes in 2018 with the implementation of the sweeping Cybersecurity Law and upgrades to surveillance technology. The law centralizes all internet policy within the Cyberspace Administration of China (CAC), strengthens obligations for network operators and social media companies to register users under their real names, requires that local and foreign companies work to "immediately stop transmission" of banned content, and compels them to ensure that all data about Chinese users is hosted within the country. The Cybersecurity Law has been followed by hundreds of new directives—an average of nearly one every two days—to fine-tune what netizens can and cannot do online. Among other steps, authorities have cracked down on the use of VPNs to circumvent the Great Firewall, leading Apple to delete hundreds of the services from its local app store.

One of the most alarming developments this year has been the uptick in state surveillance. In the western region of Xinjiang, home to the country's Uighur Muslim minority, facial recognition technology and other advanced tools are being used to monitor the local population and thwart any actions deemed to harm "public order" or "national security." Leaked documents and other evidence revealed in August suggested that as many as a million Muslims may be held in internment camps in Xinjiang, where they endure a "reeducation" process meant to forcibly indoctrinate them. Many detainees are held as a result of their nonviolent online activities.

The abuses in Xinjiang foreshadow the impact of the nascent nationwide Social Credit System, which rates citizens' "trustworthiness" by combining data on their online and offline behavior. Local activists have already reported having their freedom of movement curtailed after being blacklisted for their criticism of government policies, and the Social Credit System may lead to many more repercussions of this kind. A government website contains a list of the names and identification numbers of individuals who have "lost" their social credit, as well as up-to-date statistics on exactly how many millions of people are banned from air and rail travel. Planning documents call for the system to be expanded to businesses, which could entail de facto blacklisting of foreign companies that refuse to abide by Chinese rules on contentious political and human rights issues.

In what may or may not be a coincidence, state officials gave licenses to eight companies in 2015 to establish privately run credit platforms. Ant Financial, an affiliate of the e-commerce conglomerate Alibaba, runs a voluntary service called Sesame (Zhima) Credit, which combines aspects of the United States' FICO scores, a corporate loyalty program, and a computer game. Individuals can boost their score (ranging from

Activists of the 'Society for Threatened Peoples' in Berlin demonstrate wearing computer monitors with a portrait of Chinese President Xi Jinping on July 9, 2018, prior to a meeting between German Chancellor and Chinese Premier. (TOBIAS SCHWARZ/AFP/Getty Images)

350 to 950) by making charitable donations, purchasing products linked to good citizenship (such as diapers), and befriending others with high scores. Ant Financial has partnered with hundreds of companies and institutions to provide benefits for those with high scores, ranging from waived deposits at hotels and rental-car agencies to expedited security access at airports.

Much reporting on the issue has conflated the private and state-run systems. In practice, the Social Credit System probably poses a greater threat to civil liberties than any private initiative. But in a country where political dissent is a serious criminal offense, services like Sesame Credit can be compelled by authorities to hand over all of the data they have collected on their customers' daily lives. Sesame Credit also incorporates data from the Social Credit System into its ratings, amplifying the impact of any appearance on a government blacklist. The government will likely study the effectiveness and popularity of private credit ratings ahead of the full rollout of its own Social Credit System set for 2020.

A new flair for exporting the model under Xi

Speaking at the Chinese Communist Party Congress in October 2017, President Xi Jinping publicly outlined his plan to transform China into a "cyber superpower." He offered up the country's model of governance—including its management of the internet—as "a new option for other countries and nations that want to speed up their development while preserving their independence." But rather than simply leading by example, this year Beijing took major steps to establish its standards and practices around the world, in keeping with a detailed vision outlined not only in Xi's past speeches but also in party policy journals.

For example, users of WeChat, China's locally developed social media platform, complained of censorship even when accessing the service outside of the country. US companies like Delta, United, and American Airlines acceded to Chinese demands to list Taiwan as a part of China on their websites. The CAC blocked the hotel company Marriott's website and booking app after it included Taiwan, Hong Kong, Tibet, and Macau in a list of "countries" in a customer survey, which the agency said had "seriously violated national laws and hurt the feelings of the Chinese people." Service was unblocked after the company issued a statement asserting its support for the "sovereignty and territorial integrity of China" and distancing itself from "separatist groups." Mercedes-Benz issued a similar apology after an advertisement for the automaker on

Instagram featured a quote from the Dalai Lama, the exiled Tibetan spiritual leader.

One key avenue for China's multifaceted expansionism is the Belt and Road Initiative (BRI), a trillion-dollar international development strategy focused on infrastructure projects that enhance Chinese trade and influence in the host countries. The BRI includes a "digital Silk Road" of Chinese-built fiber-optic networks that could expose internet traffic to greater monitoring by local and Chinese intelligence agencies, particularly given that China is determined to set the technical standards for how the next generation of traffic is coded and transmitted. To this end, China has organized forums where it can impart its norms to authoritarian-leaning governments, like the 2017 World Internet Conference in Wuzhen.

China's charm offensive against internet freedom

As part of its multilateral efforts, Beijing is cultivating media elites and government ministers around the world to create a network of countries that will follow its lead on internet policy. Chinese officials have held trainings and seminars on new media or information management with representatives from 36 out of the 65 countries covered in this survey.

Beijing is cultivating media elites and government ministers around the world to create a network of countries that will follow its lead on internet policy.

Last November, China hosted a two-week "Seminar on Cyberspace Management for Officials of Countries along the Belt and Road Initiative." Visiting officials toured the headquarters of a company involved in "big data public-opinion management systems," including tools for real-time monitoring of negative public opinion and a "positive energy public-opinion guidance system."

Often the trainings are focused on a specific country. Media officials and prominent journalists from the Philippines visited China for two weeks in May 2018 to learn about "new media development" and "socialist journalism with Chinese characteristics." A similar conference for senior media staff from Thailand was described by Chinese news outlets as an opportunity for visitors to learn about "the Chinese Dream" and "the important role played by new media in domestic and international affairs," including China's development model. A three-week "Seminar for Senior Media Staff in Arab Countries" brought in representatives from Egypt, Jordan, Lebanon, Libya, Morocco, Saudi Arabia, and the United Arab Emirates.

While it is not always clear what transpires during such seminars, a training for Vietnamese officials in April 2017 was followed in 2018 by the introduction of a cybersecurity law that closely mimics China's own law. Increased activity by Chinese companies and officials in Africa similarly preceded the passage of restrictive cybercrime and media laws in Uganda and Tanzania over the past year.

Chinese companies under the spotlight

Chinese companies are playing a prominent role in the country's push for telecommunications dominance, having installed internet and mobile network equipment in at least 38 countries. Some of these firms are private enterprises and may have their own reasons for making such investments, but all are also beholden to the government and its strategic goals. State-owned China Telecom, China Unicom, and China Mobile are laying down the digital Silk Road, with fiber-optic links to Myanmar, Kyrgyzstan, and Nepal, among other countries. A company called H3C has already won contracts to build the telecommunications network for airports in Nigeria and the port of Gwadar in Pakistan. Huawei is building Latin America's largest public Wi-Fi network in Mexico, Bangladesh's 5G mobile network, and Cambodia's 4.5G service, and is advising the Kenyan government on its "master plan" for information and communication technologies.

Chinese firms have also provided high-tech tools of surveillance to governments that lack respect for human rights. In 18 of the 65 countries assessed by Freedom House, enterprises such as Yitu, Hikvision, and CloudWalk are combining advances in artificial intelligence and facial recognition to create systems capable of identifying threats to "public order." CloudWalk signed an agreement with Zimbabwe to build a national facial recognition database and monitoring system. Citizens had no say in the deal, under which Zimbabwe will send biometric data on millions of its people to China to help train CloudWalk's artificial intelligence (AI) programs to recognize faces with darker skin tones. Such collaboration and the data it provides not only enhance the Chinese government's own tech-infused policing capacity, but also renders

THE WORLD IS BUYING WHAT CHINA IS SELLING

Chinese companies are building the technological infrastructure of the 21st century, and Chinese officials are training many of their counterparts on how to use it. The table below refers to events from January 2017 until the publication of this report.

● –**Telecom Infrastructure:** Internet and mobile networking equipment installed by Chinese companies

● – **AI Surveillance:** Intelligent monitoring systems and facial recognition technology developed by Chinese companies

● – **Trainings:** Local media elites and government officials hosted in China for weeks-long seminars on new media or information management

Angola	PF	●	○	●
Armenia	F	○	●	○
Australia	F	●	○	○
Azerbaijan	PF	○	●	○
Bahrain	NF	●	○	○
Bangladesh	PF	●	○	●
Belarus	NF	●	○	●
Brazil	PF	○	○	●
Cambodia	PF	●	○	●
Canada	F	●	○	○
Cuba	NF	●	○	○
Ecuador	PF	●	●	○
Egypt	NF	●	○	●
Ethiopia	NF	●	○	●
France	F	●	○	○
The Gambia	PF	○	○	●
Georgia	F	○	○	●
Germany	F	●	●	○
Hungary	F	●	○	○
India	PF	●	○	●
Indonesia	PF	○	○	●
Iran	NF	●	○	●
Italy	F	●	○	○
Japan	F	●	○	○
Jordan	PF	○	○	●
Kazakhstan	NF	○	●	○
Kenya	PF	●	●	●
Kyrgyzstan	PF	○	●	○
Lebanon	PF	●	○	●
Libya	PF	●	○	●
Malawi	PF	●	○	●
Malaysia	PF	○	●	○
Mexico	PF	●	○	○
Morocco	PF	●	○	●
Myanmar	NF	●	○	●
Nigeria	PF	●	○	●
Pakistan	NF	●	●	●
Philippines	PF	○	○	●
Russia	NF	○	○	●
Rwanda	PF	●	●	●
Saudi Arabia	NF	●	○	●
Singapore	PF	○	●	●
South Africa	F	●	○	●
Sri Lanka	PF	●	●	●
Sudan	NF	●	○	●
Syria	NF	○	○	●
Thailand	NF	○	○	●
Tunisia	PF	●	○	○
Uganda	PF	●	○	○
Ukraine	PF	○	●	○
United Arab Emirates	NF	○	●	●
United Kingdom	F	●	○	○
Uzbekistan	NF	○	●	○
Venezuela	NF	●	●	●
Vietnam	NF	○	○	●
Zambia	PF	●	●	●
Zimbabwe	PF	●	●	●
# of countries		**38**	**18**	**36**

FOTN 2018 Status

- **F – FREE**
- **PF – PARTLY FREE**
- **NF – NOT FREE**

the companies' products more effective and attractive to foreign autocrats.

As more of the world's critical telecommunications infrastructure is built by China, global data may become more accessible to Chinese intelligence agencies through both legal and extralegal methods. In January 2018, African Union security staff reported that their computer systems had been sending confidential data back to Shanghai every day for five years. China had spent $200 million constructing the AU's new headquarters in Addis Ababa, including its computer network.

Such incidents have led to greater scrutiny of Chinese companies in democracies. In August, the United States banned government agencies and contractors from using certain products from Huawei, ZTE, and several other Chinese technology firms. Testifying before the Senate, US intelligence chiefs had warned citizens against using Huawei and ZTE products, with Federal Bureau of Investigation director Christopher Wray stating his deep concern "about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks." Australia also banned local providers from purchasing 5G equipment from Huawei and ZTE and instructed military personnel not to use WeChat on their mobile phones due to security concerns.

As more of the world's critical telecommunications infrastructure is built by China, global data may become more accessible to Chinese intelligence agencies.

How democracies can push back

Democracies have a number of options for slowing China's techno-dystopian expansionism, from tightening import and export controls to imposing sanctions on tech companies that enable human rights abuses. They can also help defend their own companies from demands to participate in China's Social Credit System or otherwise comply with antidemocratic standards and practices.

Citizens can also hold companies accountable for compromising their commitments to democratic values for the sake of access to China's lucrative market. In an internal company letter from August, some 1,400 Google employees called for greater transparency after media reports revealed plans to launch a censored search and mobile news service in China, in which users' activity would be linked to their telephone numbers. Similar internal pressure in June led the company to reevaluate its work with the US Defense Department in the field of artificial intelligence; chief executive Sundar Pichai publicly pledged not to pursue AI applications, including surveillance tools, that are likely to cause harm or contravene "widely accepted principles of international law and human rights."

As China strives to become an AI powerhouse by 2030, the moral and ethical concerns surrounding the technology deserve greater attention. Like nuclear science, AI will inevitably fall into the hands of governments that seek to use it for authoritarian ends. Democracies will face temptations as well, given the appeal of AI applications for everything from e-commerce to national security. Ensuring that government agencies and private companies abide by ethical codes will require constant vigilance by civil society, investigative journalists, and official oversight bodies, the last of which may play a key role in preventing the transfer of advanced technology that can be used for both benign and malign purposes to countries like China.

But the best way for democracies to stem the rise of digital authoritarianism is to prove that there is a better model for managing the internet. This entails tackling social media manipulation and misuse of data in a manner that respects human rights, while preserving an internet that is global, free, and secure. Democratic governments will have to devote much greater diplomatic and other resources to countering China's charm offensive on the international stage. More governments are turning to China for guidance and support at a time when the United States' global leadership is on the decline, and the acquiescence of foreign companies to Beijing's demands only emboldens the regime in its effort to rewrite international rules in its favor. If democracies fail to advance their own principles and interests with equal determination, digital authoritarianism will become an inescapable reality almost by default.

Citing fake news, governments curb online dissent

Like "terrorism," the term "fake news" has been co-opted by authoritarian leaders to justify crackdowns on dissent. Deliberately falsified or misleading content is a genuine problem, but some governments are using it as a pretext to consolidate their control over information. In the past year, at least 17 countries approved or proposed laws that would restrict online media in the name of fighting "fake news" and online manipulation.

Effectively countering disinformation and violent extremism online will require smart solutions ranging from digital literacy education to partnerships between civil society and tech companies. Yet many of the states mulling new media laws are more concerned about asserting political dominance in the online sphere than protecting their populations from false news. Governments in Belarus, Cambodia, China, Egypt, Iran, and Russia all took steps to silence independent voices, essentially arguing that only the state can be trusted to separate truth from fiction. Even democracies are at risk, as the fervor over "fake news" threatens to propel overreaching restrictions on freedom of expression and the outsourcing of key censorship decisions to ill-equipped and often opaque tech companies.

Making everyone a journalist, in countries where journalism is a crime

A number of governments are moving to regulate social media users as media outlets in order to legitimize further crackdowns on online speech. Egypt, a country that ranks third in the world for the number of journalists behind bars, passed new legislation over the summer that requires all social media users with more than 5,000 followers to procure a license from the Higher Council for Media Regulation. The law bears a strong resemblance to measures passed earlier in other countries: Cambodia now requires all websites to register with the Ministry of Information as part of a directive passed in July that also prescribed jail sentences of up to two years for spreading fake news online; some of the country's last remaining independent news sites have been shuttered or sold off as part of an ongoing crackdown on the press. In June 2017, China began implementing regulations that ban some social media accounts from posting news without a permit, while in January

Global internet user stats

Nearly **3.7 billion** people have access to the internet.

According to Freedom House estimates:

71% live in countries where ICT users were arrested or imprisoned for posting content on political, social, or religious issues.

55% live in countries where political, social, or religious content was blocked online.

48% live in countries where individuals have been attacked or killed for their online activities since June 2017.

47% live in countries where the surveillance powers of the authorities increased in the past year, threatening user rights to privacy.

47% live in countries where access to social media or messaging platforms were temporarily or permanently blocked.

42% live under governments that disconnected internet or mobile networks, often for political reasons.

An authorized rally in protest against internet censorship takes place in central Moscow. (Photo by Vladimir Gerdo\TASS via Getty Images)

2017, administrators of Telegram groups with over 5,000 followers were asked to register with authorities in Iran. Russia pioneered these tactics with a 2014 law that required the registration of blogs with over 3,000 monthly visitors as media outlets. The Russian law also made bloggers liable for the "accuracy" of their content, in a legal environment where criticism of the government is often deemed false or extremist.

India leads the world in the number of internet shutdowns, with over 100 reported incidents in 2018 alone.

Jailing dissidents for spreading false news

Many governments are enforcing criminal penalties for the publication of what they deem false news. In 2018, 13 countries prosecuted citizens for spreading false information. Rwandan blogger Joseph Nkusi was sentenced in March 2018 to 10 years in prison for incitement to civil disobedience and the spreading of rumors, having questioned the state's narrative on the 1994 genocide and criticized the lack of political freedom in the country. Police in Bangladesh arrested media activist Shahidul Alam only hours after he live-streamed a video on Facebook in which he decried a disproportionate crackdown on protesters in August. Alam faces a prison sentence of up to seven years for spreading false news against the government under the ICT Act, which has been invoked to detain dozens of social media users over the past year.

Authoritarian leaders have targeted entire news organizations under the guise of combating fake news. In Kazakhstan, online media outlets Ratel and Forbes.kz faced criminal charges of spreading false information after businessman and former top government official Zeinulla Kakimzhanov filed a complaint over stories that accused him of involvement in corruption. Lawmakers in the Philippines proposed criminalizing the dissemination of false news with malicious intent. President Rodrigo Duterte has attacked the investigative media site Rappler as a "fake news outlet" and sought to shut it down in January over alleged foreign funding violations.

Shutting down internet access

While more repressive governments tend to use false news and hate speech as an excuse to curb dissent or independent reporting, inflammatory lies on social media remain an urgent problem in many countries, and some have responded by cutting off access entirely.

Authorities in India and Sri Lanka temporarily shut down mobile networks or blocked social media apps during riots and protests, claiming that the measures were necessary to halt the flow of disinformation and incitement to violence. In March, online rumors that Muslims were trying to sterilize Sinhalese Buddhists in Sri Lanka led a group of Buddhist men to beat a Muslim man and set fire to his shop. In the ensuing weeks, extremists used Facebook to implore followers to "rape without leaving an iota behind" and "kill all Muslims, don't even save an infant." Authorities reacted by blocking four social media platforms that they said were amplifying hate speech.

India leads the world in the number of internet shutdowns, with over 100 reported incidents in 2018 alone. Users in the state of Tamil Nadu shared a video showing a child being kidnapped by a masked motorcyclist on WhatsApp, along with an audio message warning that 200 "Hindi-speaking" child kidnappers were entering the state. The video was actually from a public-service announcement against child kidnapping in Karachi, Pakistan. Mobs killed at least two people and physically assaulted several others who were mistaken for kidnappers.

Shutdowns are a blunt instrument for interrupting the spread of disinformation online. By cutting off service during such incidents, governments often deny entire cities and provinces access to communication tools at a time when they may need them the most, wheth-

er to dispel rumors, check in with family members, or avoid dangerous areas. In practice, shutdowns serve as a substitute for more effective policymaking to counter online manipulation without disproportionate restrictions on freedom of expression and access to information.

Outsourcing censorship to social media companies

Even in democracies with a high level of digital literacy, it is often hard to distinguish between trusted sources from one's own community and information created by a fake-news factory in Macedonia, a troll army in Russia, or an intelligence unit in Iran. Policymakers have focused their ire on tech companies for failing to keep fraudulent content off their platforms, or conversely, for taking down posts or curating news in a way that seems to privilege certain political leanings. US president Donald Trump—who popularized the term "fake news" as a smear for outlets that report critically on his policies—claimed in August that Google search results for the term "Trump News" are "rigged" to promote negative articles. Such controversies demonstrate the challenges faced by tech companies that are compelled to make difficult decisions about what constitutes appropriate speech. The task is especially fraught given that they lack the transparency, accountability, and public input associated with governmental or judicial decision-making in a democracy.

Some democracies have increased companies' legal liability for third-party content appearing on their platforms, hoping that this will force them to police illegal speech. The European Union is currently mulling rules that would require social media companies to remove content that violates the laws of its 28 member states. The initiative came as Germany's Social Media Enforcement Law (known as NetzDG) came into force last October, obliging social media platforms with over two million local users to monitor and remove "obviously illegal content" or face fines of up to €50 million. Dozens of different German laws contain provisions limiting certain forms of expression, from defamation of religion to depictions of violence. It is left to the companies to interpret these statutes and take action, affecting users without any due process or prior approval from a court. Imposing similar requirements on tech companies across the EU would likely result in greater confusion and missteps that could unduly harm freedom of expression.

Protections against intermediary liability are also eroding on the other side of the Atlantic. There is ongoing pressure in the United States to rescind "safe harbor" protections in Section 230 of the Communications Decency Act. Without the provision, companies that make mistakes when attempting to remove banned content could be held liable for allowing illegal activities on their platforms, encouraging them to err on the side of censorship rather than protecting legitimate expression.

The promise of broad collaboration to counter disinformation

More constructive solutions arise out of collaboration among civil society groups, governments, and tech companies. Italian lawmakers have partnered with journalists and tech firms to pilot a nationwide curriculum on spotting online manipulation. In the US, several states have passed or proposed laws to increase media literacy programs in local schools. The civic education initiatives include efforts to teach students to evaluate the credibility of online media sources and identify disinformation. Many of the laws require state education officials to engage with media literacy organizations in the creation of their curriculums, and are based on model legislation backed by civil society experts. WhatsApp, which is owned by Facebook, is working together with seven organizations in India to draft a digital literacy training program for its users.

Some democracies have increased companies' legal liability for third-party content appearing on their platforms, hoping that this will force them to police illegal speech.

Social media companies are also working with civil society to identify disinformation on their platforms. Facebook's collaboration with DFRLab at the Atlantic Council in the United States led to the discovery of fake accounts controlled by entities in Russia and Iran. Comprova, an initiative by the nonprofit First Draft and the Brazilian Association of Investigative Journalists (ABRAJI), brings together 24 Brazilian news outlets to identify and counter disinformation ahead of the country's elections. The project marks the first time a journalists' association has been granted access to WhatsApp's business API (application programming interface), which will improve the group's ability to reach audiences on the platform.

Lebanese people gather to stage a protest at Samir Kassir Square in Beirut after security forces took social media users into police custody in July 2018. (Photo by Wassim Samih Seifeddine/Anadolu Agency/Getty Images)

Through a partnership with Facebook, the Argentinean organization "Chequeado" runs a bot that automatically matches media claims on the network with fact-checking research.

These examples of cooperation show how government, civil society, and tech companies can play a productive and healthy role in protecting the digital sphere from manipulation. Governments should use caution when asking the private sector to perform a task that they are unwilling and unable to perform themselves: Proactively or preemptively assessing the legality of billions of online posts would require massive additional resources and constitute a worrying intrusion of the government into social media, where the line between public and private communication is often blurred. But forcing private companies to do the same—without proper safeguards—can also damage individual rights, reducing transparency and due process while allowing public officials to shift the blame for any abuses.

Protecting the digital commons from manipulation without harming human rights will require innovation and increased investments from states, tech companies, and civil society alike.

Such problems can be mitigated if local laws on illegal content respect international human rights norms, companies' content moderation practices are transparent, and users have an avenue for appeal against improper deletions. Whenever possible, companies should establish a mechanism for input from civil society experts in the countries where they operate. Social media firms can also incorporate democratic principles into their decision-making by promoting public participation and open deliberation, ensuring that policies are implemented in a way that does not violate the human rights of their users.

For democracy to thrive, citizens must have freedom of expression and access to a public forum that allows rational discourse. Protecting the digital commons from manipulation without harming human rights will require innovation and increased investments from states, tech companies, and civil society alike.

Authorities demand control over personal data

In many ways, the internet erases borders. But as governments recognize the importance of the data flowing in and out of their countries, they are establishing new rules and barriers in the name of national sovereignty, allowing officials to control and inspect such information at will. Governments in 18 out of 65 countries have passed new laws or directives to increase state surveillance since June 2017, often eschewing independent oversight and exposing individuals to persecution or other dangers in order to gain unfettered access.

Some of these countries now require that tech firms store their citizens' data on local servers, with the stated intention of either making the records more accessible to national security agencies or protecting them from theft or exploitation by others. China, Russia, Vietnam, Nigeria, and Pakistan have already instituted data localization requirements. The government in India, home to the world's second-largest population of internet users after China, has proposed similar rules on privacy grounds. Although the country scored a major victory for internet freedom when its Supreme Court ruled in August 2017 that Indians have a fundamental right to privacy, it has also been plagued by security breaches.

On the surface, data localization appears to be a rational response to such concerns, but it makes little difference to transnational hackers whether Indians' personal data are located in Bangalore or Boston. Moreover, Indian authorities have already proven to be poor custodians of citizens' information. In 2018, researchers discovered a number of breaches in India's national biometric database, named Aadhar, leaving the data of 1.1 billion people vulnerable to identity thieves and other malicious actors. The scandal demonstrated the urgent need for reforms to the country's data protection framework, beyond simply requiring that data be stored locally.

The Kremlin's intrusive gaze

Russia took significant steps over the past year to increase data sovereignty. Lawmakers passed restrictions on virtual private networks (VPNs) in July 2017, ostensibly to prevent users from accessing banned sites that are hosted outside the country. A subsequent bill introduced this year includes fines for VPN companies that allow such access. Other new provisions from the past year require communication apps to register users under their real names, so that they can be identified by law enforcement agencies. And antiterrorism provisions that came into force in July require telecommunications firms and other companies to store the content of users' online communications for up to six months, in addition to metadata, and provide the Federal Security Service (FSB) with unfettered access to both.

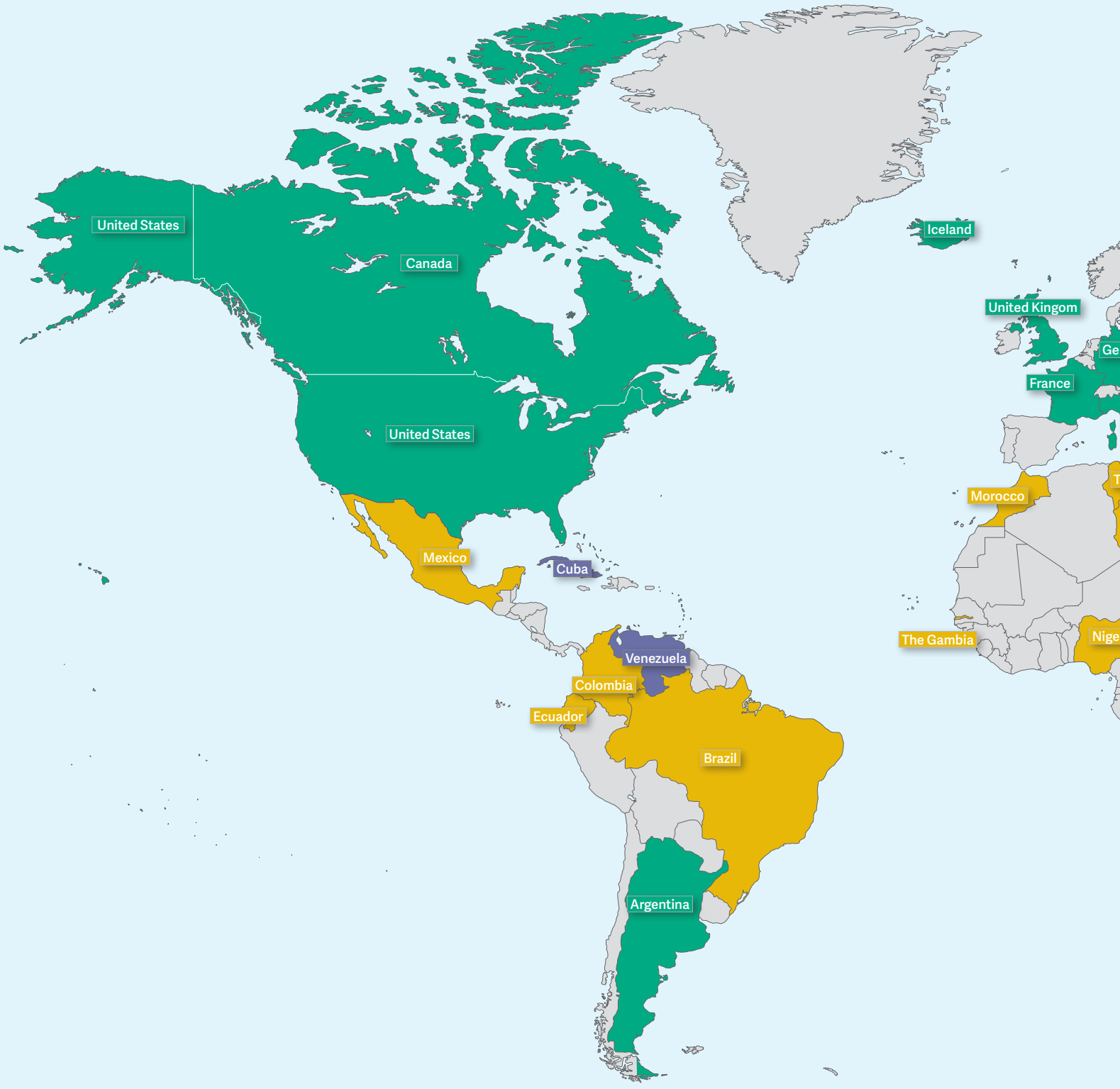
Russian authorities blocked Telegram due to its refusal to make encrypted data accessible to the FSB.

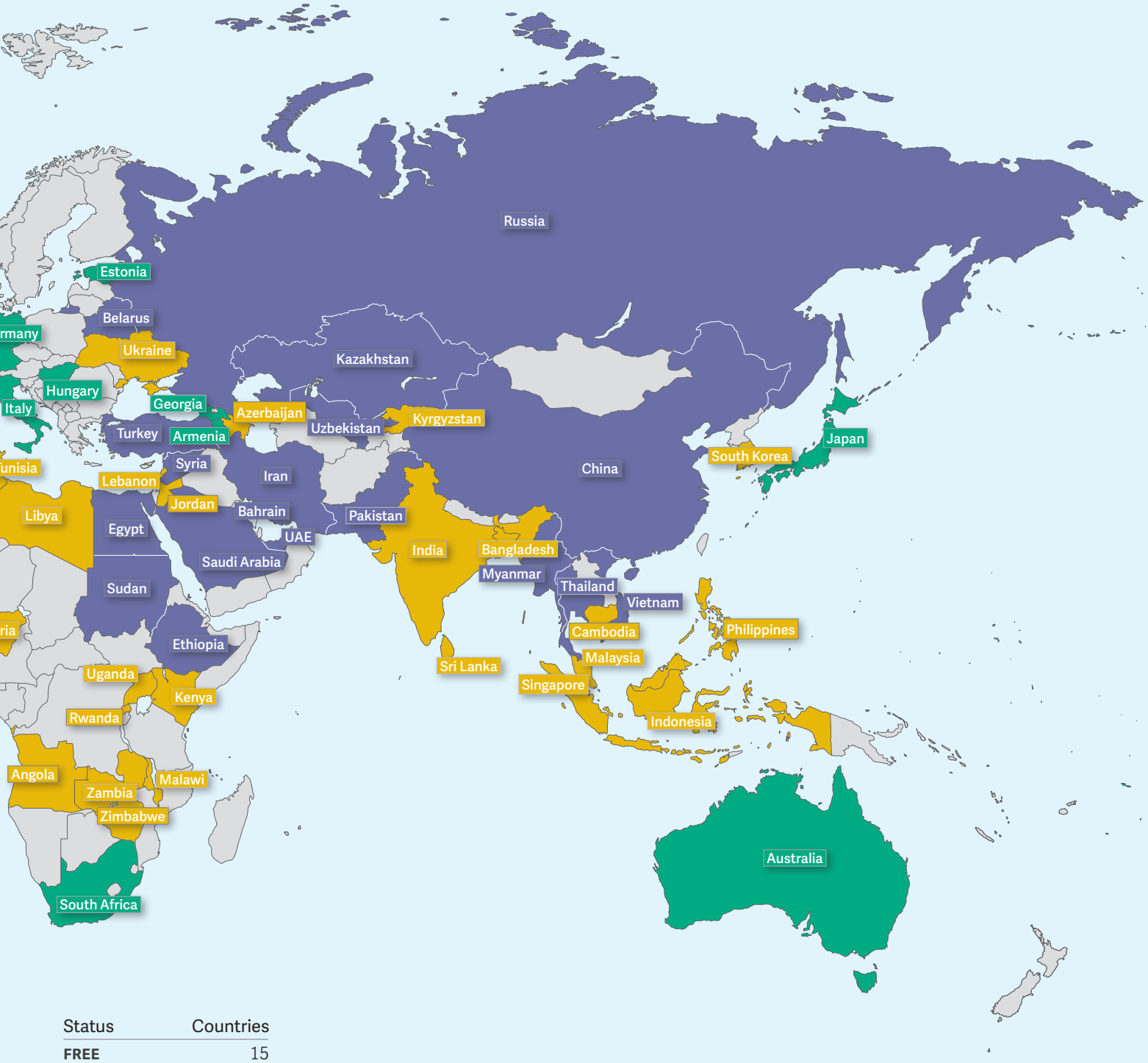
The most high-profile example of Russia's enforcement of data sovereignty involves Telegram. The secure messaging app was widely used to hold private conversations in what is otherwise a heavily policed environment. In April, authorities blocked the service due to its refusal to comply with laws that require tech companies to make encrypted data accessible to the FSB. When Telegram used various methods to overcome the initial blocking, the state internet regulator ordered the obstruction of at least 18 million IP (internet protocol) addresses in an escalating game of whack-a-mole, bringing down news sites, smart television sets, and even airline ticketing systems in the process. Telegram's self-exiled founder, Pavel Durov, had previously sold off VKontakte, Russia's most popular social media company, amid growing pressure to provide the government with information on its users. With Telegram, he vowed to create new social media technology that would be far more resistant to state control.

Intelligence agencies afraid of going dark

Though their motives and methods differ from those of the Kremlin, democratic governments are voicing their own determination to overcome encryption when national security is at stake. Government ministers of the so-called Five Eyes intelligence alliance—Australia, Canada, New Zealand, the United Kingdom, and the United States—released a statement calling on companies to "voluntarily establish lawful access

FREEDOM ON THE NET 2018





Status	Countries
FREE	15
PARTLY FREE	30
NOT FREE	20
Total	**65**

Freedom on the Net 2018 assessed 65 countries around the globe.

solutions" for encrypted content or face possible government attempts to break into their systems. The latest draft surveillance bill in Australia contains vague language that could require companies to build "back doors" into their encryption technology. Such a policy would effectively create security vulnerabilities in the companies' services, driving away users and facilitating intrusions not just by friendly governments, but by hostile powers and criminals as well.

The governments of France, Germany, Hungary, and the United Kingdom have also ramped up the surveillance powers of their intelligence services with the aim of disrupting terrorist networks. While this is intended to protect citizens' safety, it often weakens crucial judicial oversight meant to protect their basic rights. Italy passed a law in November 2017 that requires telecommunications operators to store telephone and internet data for up to six years, despite a 2014 EU Court of Justice ruling that such rules constituted a disproportionate infringement on privacy.

Democratic governments are voicing their own determination to overcome encryption when national security is at stake.

The privacy policy update felt around the world

In response to fears about ubiquitous collection and the inherent insecurity of personal data, many countries are enacting legislation that grants individuals the right to control how their data are collected, processed, and shared by public and private entities. At least 15 countries considered data protection laws since June 2017, and at least 35 already have a data protection law on the books.

The data protection laws that have been proposed or passed in Argentina, Brazil, and Indonesia bear a strong resemblance to the EU's General Data Protection Regulation (GDPR), which came into effect in May 2018.

The GDPR requires data holders to obtain more meaningful consent, increase transparency about what data are collected and why, and provide a way for users to download, transfer, or delete their information.

It is not a silver bullet for digital rights. The regulation does not apply to matters of national security and defense, thus failing to curtail rampant data collection by governments. Uncertainties remain over how several articles will be implemented in practice, such as a provision that could allow a company's "legitimate interests" to supersede a person's right to privacy. And the rules incorporate the EU's problematic "right to be forgotten," under which public figures have attempted to delete articles or data they deem to be unflattering.

Nevertheless, the GDPR is one of the most ambitious attempts to regulate data collection in the 21st century. It applies to all companies and organizations that process data on Europeans, compelling firms around the world to change their privacy policies and terms of service before the implementation deadline. Numerous data-mining companies simply halted their operations in an implicit admission that their practices could not withstand scrutiny under the new rules.

The GDPR also created a framework for the free movement of personal data within the EU's 28 member states, and in any other country that institutes a high level of personal data protection. EU officials have moved to lift any data localization requirements within the bloc, such as those previously put in place by Germany. The EU has entered talks with Japan to allow for frictionless data exchanges with that country. However, an existing deal with the United States, known as Privacy Shield, has come under increased pressure this year from members of the European Parliament who worry that EU citizens' data are not afforded the same protections when processed in the US.

Protecting user data on a global internet

Governments, private companies, and researchers are increasingly hungry for large amounts of personal information, using it for purposes ranging from political repression to the development of artificial intelligence algorithms. Individuals often have few options for resisting this demand, short of disengaging from major aspects of modern life.

Rather than forcing users to make such a stark choice, governments and technology companies should strive to increase transparency regarding how personal data are used, enable data portability between platforms, and allow people to review and delete all data collected about them—steps that some of the largest companies have already taken.

One innovative national model can be found in Estonia, a country that tied with Iceland for the best internet freedom score in this survey. Its X-Road platform for

Technicians collect biometric data from a girl as part of the Aadhar Card program in New Delhi, India. In 2018, researchers discovered a number of breaches in the national Aadhar database. (Photo by Priyanka Parashar/Mint via Getty Images)

secure data sharing runs on an Estonian blockchain technology called KSI, through which all incoming and outgoing transactions are authenticated and encrypted. Among other benefits, citizens are notified when their data files are accessed by government agencies, except in cases of ongoing investigations. Given Estonia's strong legal framework for privacy rights, the system provides greater protections than in countries where citizens' data is stored unencrypted on disparate servers, with no mechanism for informing them about who possesses the information or how it is being used.

In 2018, Estonia announced plans to expand the X-Road platform beyond its borders. This step, like the EU's GDPR, stems from a basic recognition that open societies and international tech companies need to ensure the protection of data outside rigid national frameworks if they are to preserve a free and global internet. Any bona fide data protection system should give individuals the power to control their own personal information while also ensuring that the internet remains borderless.

Any bona fide data protection system should give individuals the power to control their own personal information while also ensuring that the internet remains borderless.

Recommendations

For Policymakers

- **Ensure that all internet-related laws and practices adhere to international human rights law and standards.** National governments should establish periodic reviews to assess whether their laws and practices regarding internet freedom conform to the principles outlined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Any undue restrictions on internet freedom—including the blocking of political websites, internet shutdowns, arrests for nonviolent speech, or extralegal surveillance—should cease immediately.

- **Enact strong data protection laws to provide greater transparency and control over personal data.** Policymakers should ensure that all personal data—stored either by companies or by governments—are processed according to strict principles. Individuals should have control over their information and the right to access it, delete it, and transfer it to the providers of their choosing. Private companies should be compelled to disclose how they use customer data in non-technical language, and to notify customers in a timely fashion if their data are compromised. Governments should have the right to access personal data only in limited circumstances as prescribed by law and subject to judicial authorization, and only within a specific time frame.

- **Include human rights safeguards in national strategies on artificial intelligence (AI).** As policymakers consider how AI can advance national priorities and improve citizens' lives and security, they should ensure that all proposed research and development plans include a thorough assessment of any potential effects on human rights, including the rights to privacy and free expression. Human rights assessments for the technologies in question should be made available to the public.

- **Fund rapid response capacity to counter attacks on internet freedom.** A rapid-response fund to address internet freedom emergencies—such as internet shutdowns, blocking of independent news sites, or the introduction of draconian censorship laws—would allow swift deployment of resources to local activists and other front-line defenders. The fund could be used, for example, to provide additional capacity when censorship circumvention tools face a sudden flood of demand at times of political tension and unrest.

- **Impose sanctions—such as freezing of assets—on foreign tech companies involved in human rights abuses.** For example, companies that knowingly provide surveillance systems used for repressive crackdowns in places like Xinjiang should face economic penalties. In the United States, the Global Magnitsky Act allows for targeted sanctions on "any entity not organized solely under the laws of the United States or existing solely in the United States," which could include private companies. Countries with similar laws should robustly enforce them, and legislatures in countries without such laws should seek to pass them.

- **In the United States, reintroduce and pass the Global Online Freedom Act (GOFA).** GOFA, which would impose penalties on countries that restrict internet freedom, was introduced in every U.S. Congress from 2006 to 2014 but never passed. It would direct the Secretary of State to designate internet-restricting countries; prohibit the export to those countries of any items that could be used to carry out censorship, surveillance, or internet freedom restrictions; and require internet service companies operating in internet-restricting countries to disclose as part of their annual reporting what they are doing to protect human rights and freedom of information. Other countries should consider adopting legislation with similar provisions.

For the Private Sector

- **Adhere to the UN Guiding Principles on Business and Human Rights.** Companies should commit to respecting the human rights of their users and addressing any adverse impact that their products might have on human rights. As part of this effort, they should conduct periodic assessments to fully understand how their products and actions might affect rights like freedom of expression or privacy. Upon completion of these assessments, the companies should develop actionable plans to remedy any evident or potential harm.

- **Conduct human rights impact assessments for new markets and commit to doing no harm.** International companies should not seek to operate in countries where they know they will be forced to violate international human rights principles. They should carefully weigh the consequences of entering new markets,

whether this means building tools that prevent citizens from exercising their rights to free expression, turning citizen data over to governments with poor human rights records, or providing surveillance or law enforcement equipment that is likely to be used to violate user rights.

- **Grant users control over their information and ensure that it is not being misused.** Companies should be transparent regarding what data they collect and how they are used. Individuals should have the ability to move or delete their data without significant hurdles. Companies also need to ensure that user data are not being used or shared in ways that were not explicitly authorized by the users.

- **Ensure fair and transparent content moderation practices.** In order to fairly and transparently moderate public posts within their platforms and services, private companies should do the following: (1) Clearly and concretely define what speech is not permissible in their guidelines and terms of service. (2) If speech needs to be restricted, when appropriate, consider less invasive actions before restricting speech outright, such as warning users that they are violating terms of service and adjusting algorithms that might unintentionally promote disinformation or incitement to violence. (3) Ensure that content removal requests by governments are in compliance with international human rights standards. (4) Publish detailed transparency reports on content takedowns—both for those initiated by governments or for those undertaken by the companies themselves. (5) Provide an avenue for appeal for users who believe that their speech was unduly restricted.

- **Engage in continuous dialogue with local civil society organizations.** Companies should seek out local expertise on the political and cultural context in markets where they have a presence or where their products are widely used. These consultations with civil society groups should inform the companies' approach to content moderation, government requests, and countering disinformation, among other things.

- **Label automated "bot" accounts.** Recognizing that bots can be used for both helpful and harmful purposes, and acknowledging their role in spreading disinformation, companies should strive to provide clear labeling for suspected bot accounts. Although today's technology allows reasonably high accuracy in bot recognition, companies should also establish transparent remedial mechanisms to remove the bot designation from any account that may have been mislabeled.

- **Use internal expertise to help counter Chinese state censorship and protect users.** The private sector should assist users in China by developing accessible tools that keep pace with innovations by the Chinese government and complicit Chinese firms. For example, leading international companies could develop mobile-phone applications that enhance digital security, enable sharing of images in a way that evades AI-driven censorship, and incorporate circumvention capabilities into apps focused on other services.

For Civil Society

- **Partner with the private sector on fact-checking efforts.** Activists around the globe should create or expand the current projects dedicated to fact-checking news and other potentially viral online content. They should collaborate with major tech companies to help flag news or content that might spread quickly and have a particularly negative impact on democratic processes like elections.

- **Work with scholars to examine how disinformation spreads and why people are likely to share it.** This type of research could help improve understanding of the technical and psychological drivers of disinformation and inform strategies for combating it.

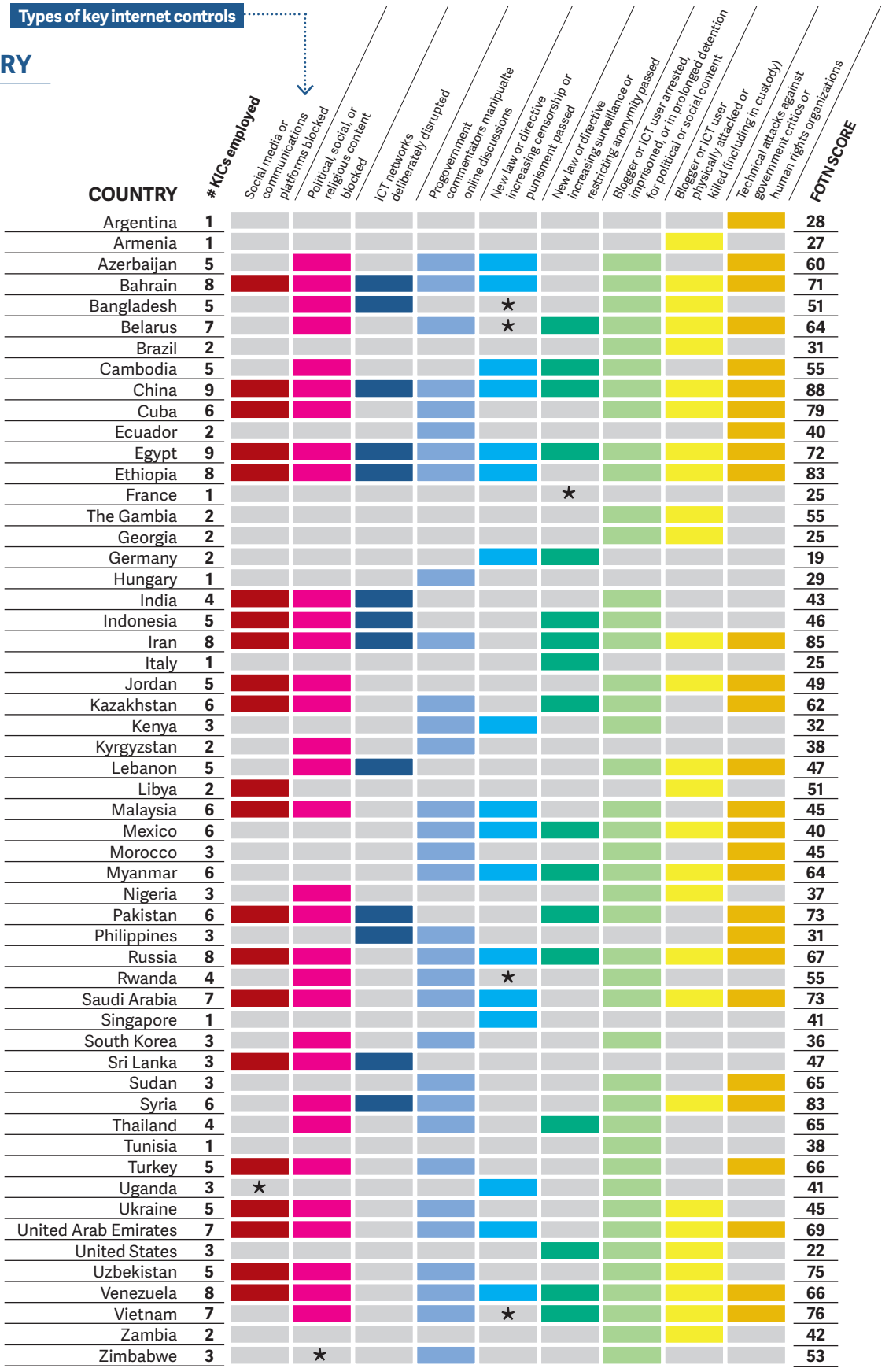
- **Monitor home countries' collaboration with Beijing and Chinese firms.** As the effects of Chinese government internet controls expand beyond China's borders, civil society groups throughout the world should vigilantly monitor their own countries for any emerging investments, infrastructure developments, official trainings, technology sales, and user data transfers related to China. They should expose any evidence of bilateral collaboration that could result in violations of internet freedom or human rights and urge their governments to resist the temptation of adopting Chinese-style censorship or surveillance methods.

- **Continue to raise awareness about government censorship and surveillance efforts.** Civil society groups globally should engage in innovative initiatives that inform the public about governments' censorship and surveillance efforts, imprisoned journalists and online activists, and best practices for protecting internet freedom. Existing studies and surveys have shown that when users become more aware of censorship, they often take actions that enhance internet freedom and protect fellow users.

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 2017 to May 2018; cells with an asterisk (*) represent events that occurred after the coverage period until September 2018, when the report was sent to print. The Key Internet Controls reflect restrictions on political, social, or religious content.

Types of key internet controls



NO KEY INTERNET CONTROLS OBSERVED

	FOTN Score
Angola	40
Australia	21
Canada	15
Colombia	31
Estonia	6
Iceland	6
Japan	25
Malawi	39
South Africa	25
United Kingdom	23

LARGEST FIVE-YEAR DECLINES

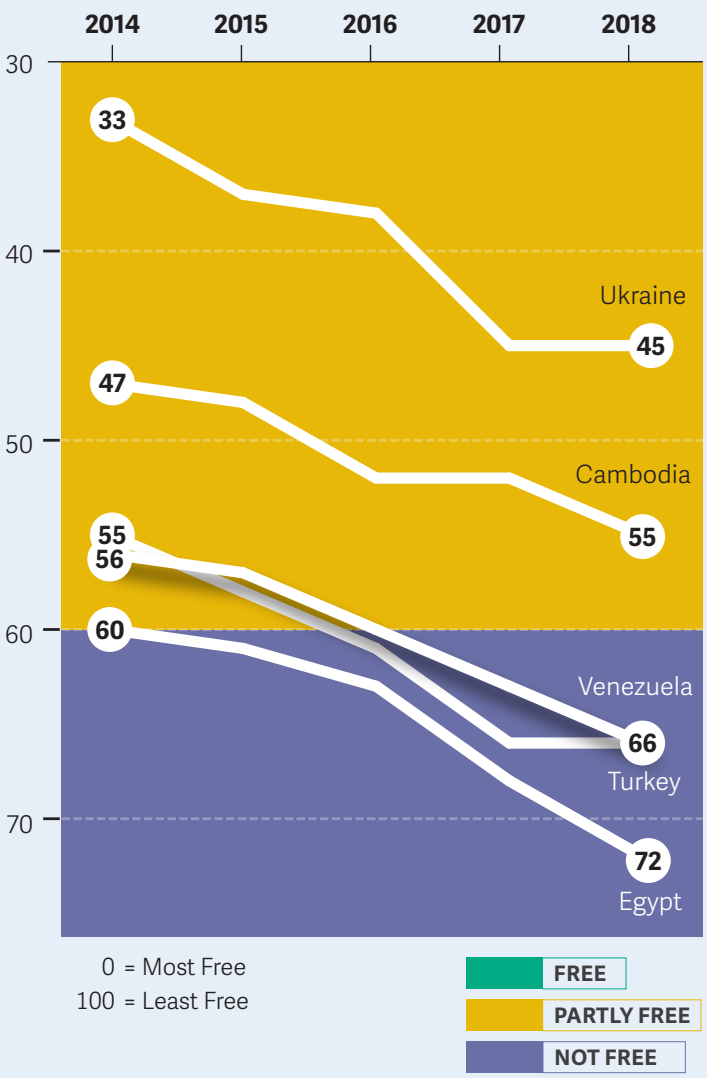
Of the 65 countries covered by *Freedom on the Net*, these five experienced the steepest deterioration in internet freedom over the last five years.

Under authoritarian prime minister Hun Sen, **Cambodia** intensified its crackdown on online dissent. Amendments to the Telecommunications Law and penal code, passed respectively in 2015 and 2018, resulted in an uptick in arrests for political commentary on social media and news sites. Self-censorship increased as activists and ordinary users alike feared reprisals amid widespread government surveillance. In the lead-up to the July 2018 general elections, the ruling Cambodian People's Party ensured its victory by intimidating and arresting political opponents, and censoring their activities online.

In **Venezuela**, Nicolás Maduro clung to power through ever-desperate and draconian curbs on digital freedoms, even as citizens' access to the internet was sharply reduced due to effects of the country's economic crisis. Once connected, they encounter a digital landscape where critical media sites are blocked, and political speech on social media sites can incur hefty penalties. Online journalists who fall afoul of authorities risk arbitrary detention. A new anti-hate speech law, carrying prison sentences of up to 20 years for spreading allegedly hateful messages on social networks, is just one of the latest tools to silence dissent.

Ukraine struggled to protect citizens' internet freedom amid the ongoing conflict with Russian-backed separatists and information war with the Kremlin. President Petro Poroshenko blocked several widely used Russian tech platforms on national security grounds in 2017; meanwhile, social media users faced jail time for nonviolent speech under measures outlawing "calls for extremism or separatism." Those within the occupied territories struggled with connectivity, while journalists faced technical attacks and physical violence on both sides of the conflict.

In **Egypt**, President Abdel Fattah al-Sisi has overseen an unprecedented crackdown on internet freedom since taking power in 2014. Authorities jailed prominent figures for their digital activism, having outlawed the country's Islamist, secular, and even military-led opposition movements as an affront to Sisi's power. Individuals have been sentenced to lengthy prison terms for absurd "offenses," including sharing satirical memes and describing instances of sexual harassment. Censorship has escalated dramatically, with the number of blocked websites rising from 2 in 2015 to over



500 in 2018, including the websites of independent media outlets and human rights organizations.

Internet freedom declined in **Turkey** under the authoritarian tenure of President Recep Tayyip Erdoğan. The ruling Justice and Development Party sought every pretext to curb civil liberties online, in response to antigovernment protests, corruption scandals, terrorist attacks, and a 2016 coup attempt. Authorities used antiterrorism laws to arrest tens of thousands of citizens for criticizing the government's crackdown on human rights. Social media companies were left with no choice but to censor nonviolent political commentary as a condition of doing business in the country, while Wikipedia was blocked entirely for failing to comply with the government's heavy-handed orders.

GLOBAL RANKINGS

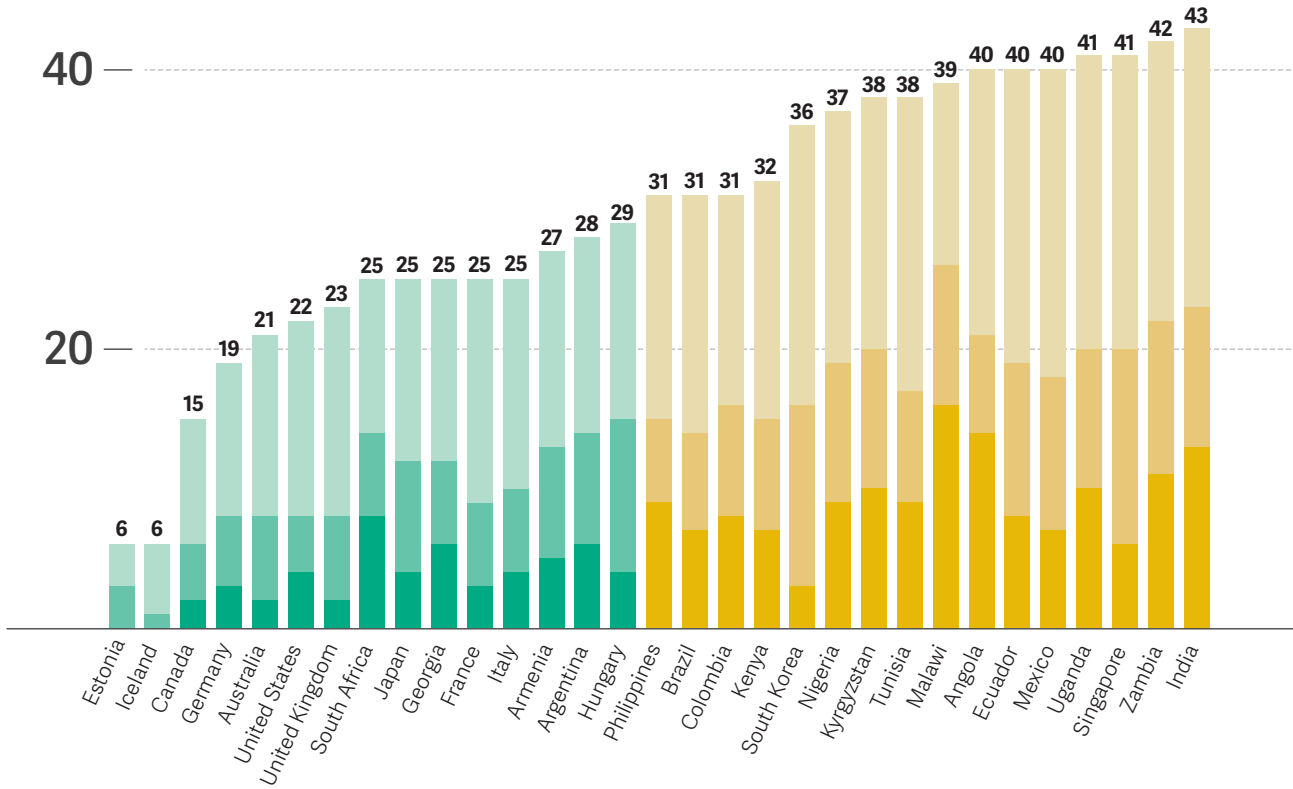
Freedom on the Net measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of FREE (0-30 points), PARTLY FREE (31-60 points),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

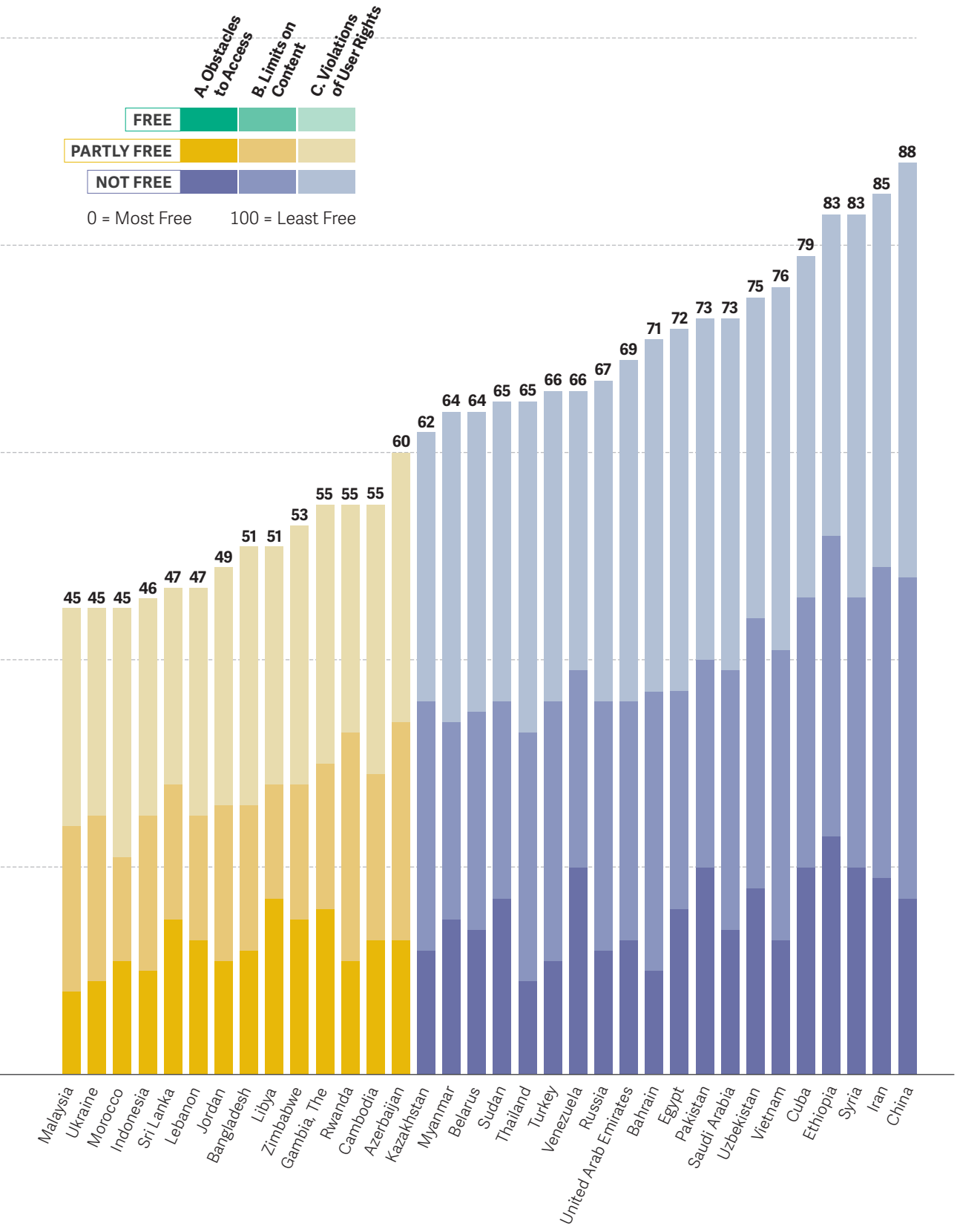
Ratings are determined through an examination of three broad categories:

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
45 45 45 46 47 47 49 51 51 53 55 55 55 60 62 64 64 65 65 66 66 67 69 71 72 73 73 75 76 79 83 83 85 88
Malaysia
Ukraine
Morocco
Indonesia
Sri Lanka
Lebanon
Jordan
Bangladesh
Libya
Zimbabwe
Gambia, The
Rwanda
Cambodia
Azerbaijan
Kazakhstan
Myanmar
Belarus
Sudan
Thailand
Turkey
Venezuela
Russia
United Arab Emirates
Bahrain
Egypt
Pakistan
Saudi Arabia
Uzbekistan
Vietnam
Cuba
Ethiopia
Syria
Iran
China

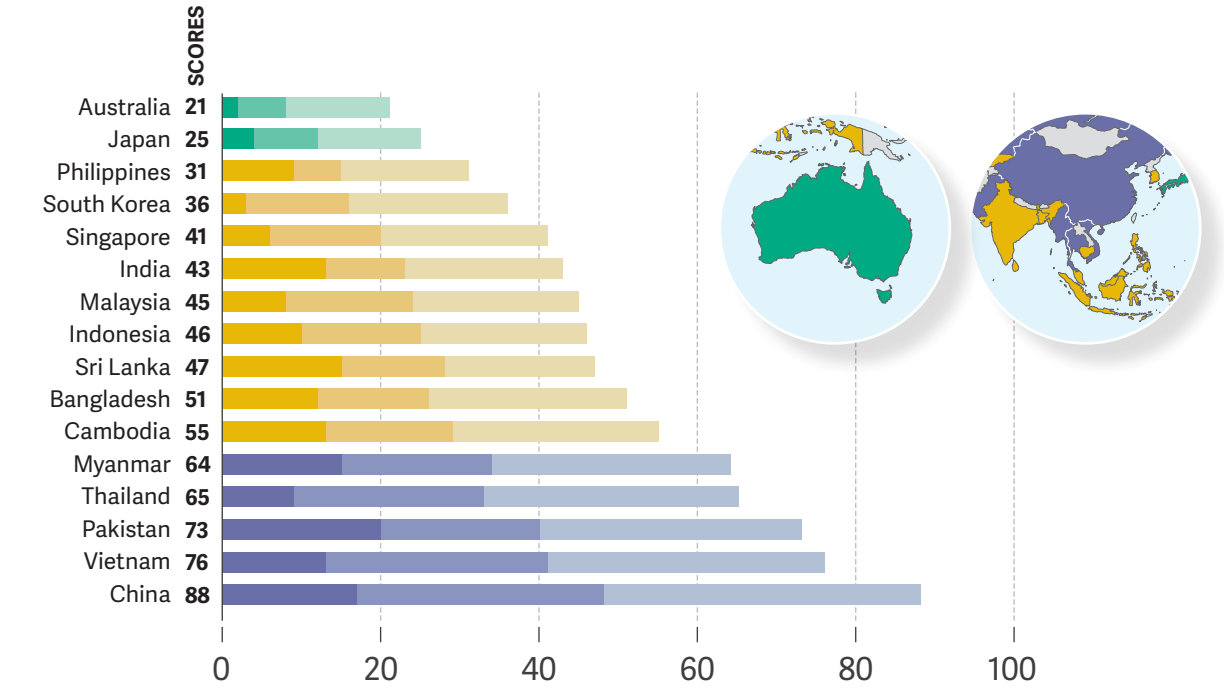
REGIONAL RANKINGS

Freedom on the Net 2018 covers 65 countries in six regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

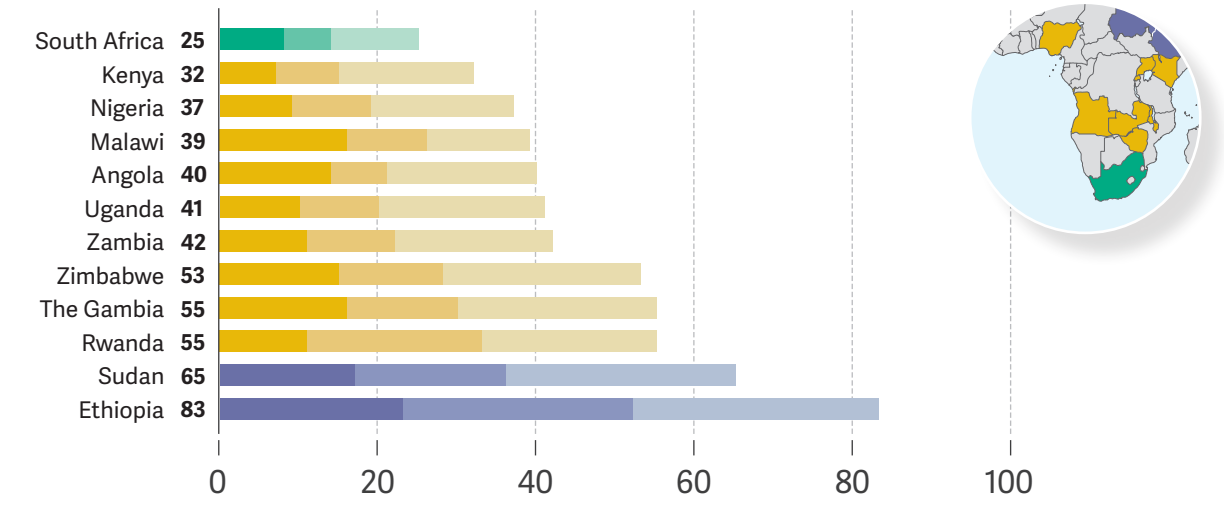
A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights

0 = Most Free
100 = Least Free

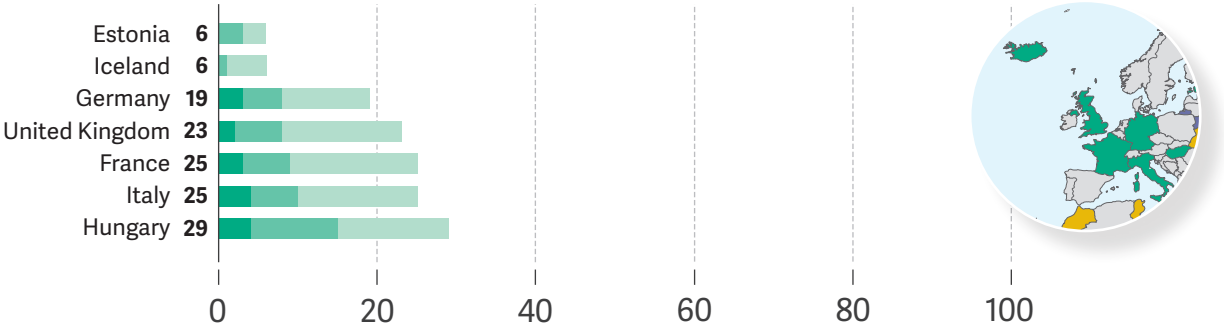
Asia-Pacific



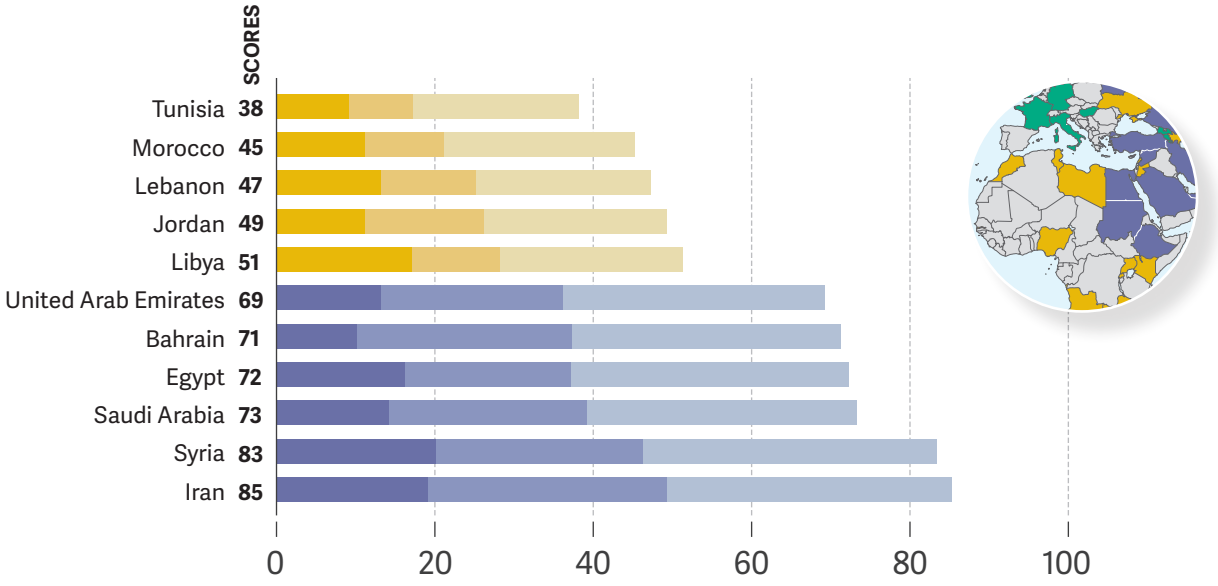
Sub-Saharan Africa



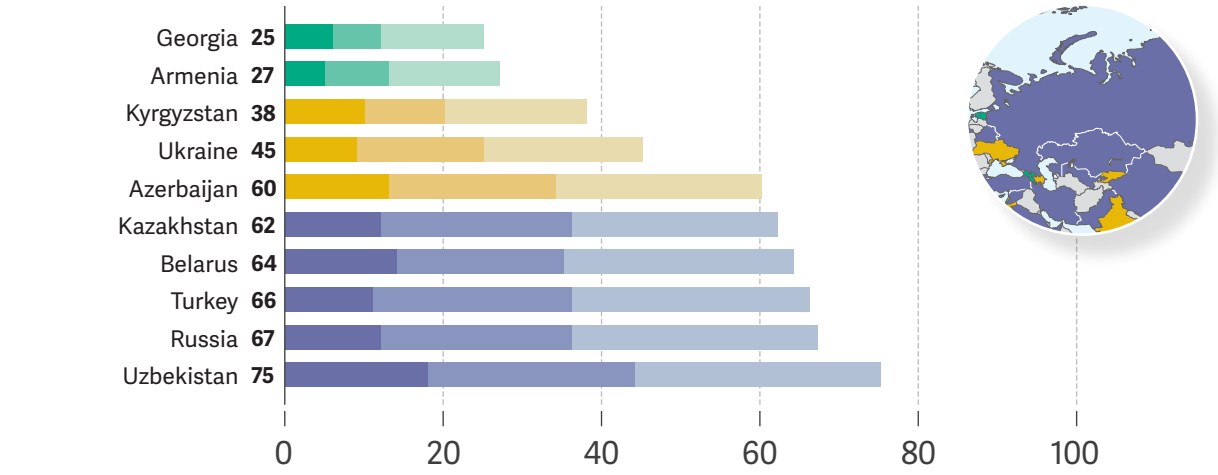
Europe



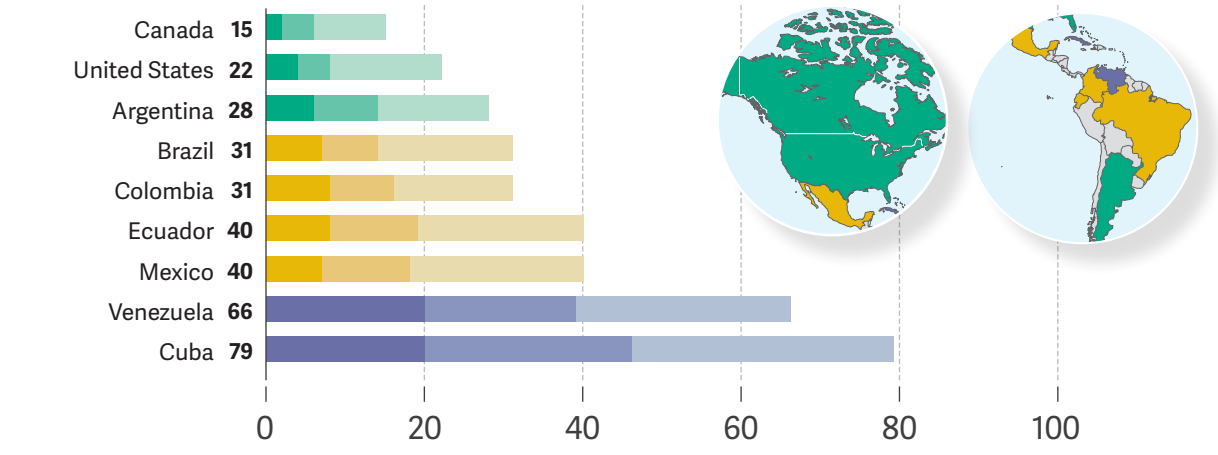
Middle East and North Africa



Eurasia

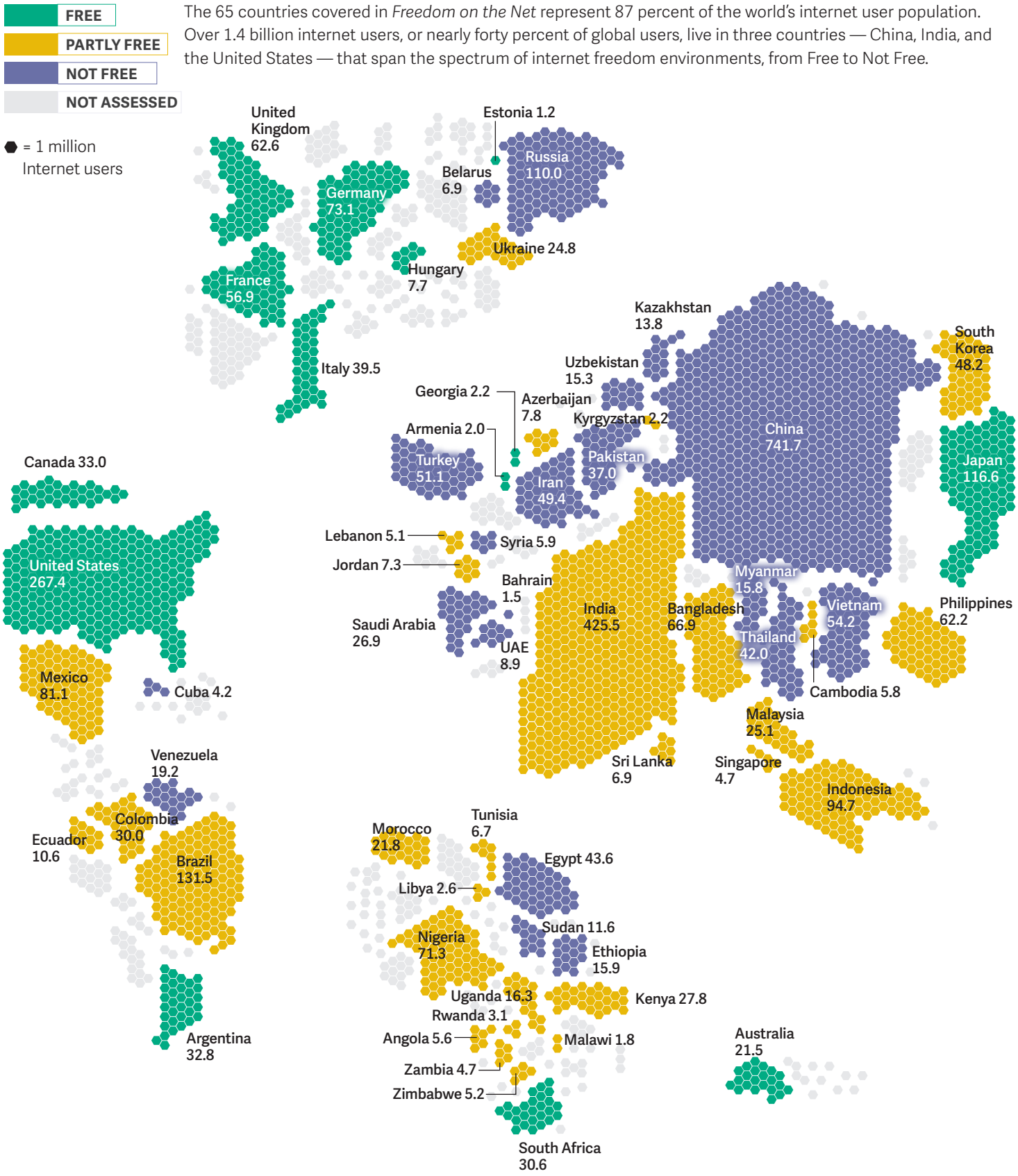


Americas



DISTRIBUTION OF GLOBAL INTERNET USERS BY COUNTRY AND FOTN STATUS

The 65 countries covered in *Freedom on the Net* represent 87 percent of the world's internet user population. Over 1.4 billion internet users, or nearly 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.



Securing internet freedom against the rise of digital authoritarianism is fundamental to protecting democracy.

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

111 John Street, Suite 810
New York, NY 10038

www.freedomhouse.org
facebook.com/FreedomHouseDC
@FreedomHouse
@FreedomOnTheNet
202.296.5101 | info@freedomhouse.org