Freedom House

FREEDOM ON THE NET 2019

The Crisis of Social Media

FREEDOM ON THE NET 2019

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), the New York Community Trust, Google, Internet Society, and Verizon Media.

The following people were instrumental in the research and writing of this report: Mai Truong, Amy Slipowitz, Isabel Linzer, and Noah Buyon. Tyler Roylance, Shannon O'Toole, and Chris Brandt edited the report. Jessica White and Sarah Cook served as advisers on Latin America and China, respectively. Alexander Rochefort provided research assistance.

This booklet is a summary of findings for the 2019 edition of *Freedom on the Net*. Narrative reports on the 65 countries assessed in this study and a full list of contributors can be found on our website at **freedomonthenet.org**.

ON THE COVER

A protester wearing a Guy Fawkes mask holds up a placard during a demonstration to mark the global "The Day We Fight Back" protest against mass surveillance outside the Supreme Court in Manila, Philippines. Credit: NurPhoto/Corbis via Getty Images.

Freedom House

The Crisis of Social Media

What was once a liberating technology has become a conduit for surveillance and electoral manipulation.

by Adrian Shahbaz and Allie Funk

Internet freedom is increasingly imperiled by the tools and tactics of digital authoritarianism, which have spread rapidly around the globe. Repressive regimes, elected incumbents with authoritarian ambitions, and unscrupulous partisan operatives have exploited the unregulated spaces of social media platforms, converting them into instruments for political distortion and societal control. While social media have at times served as a level playing field for civic discussion, they are now tilting dangerously toward illiberalism, exposing citizens to an unprecedented crackdown on their fundamental freedoms. Moreover, a startling variety of governments are deploying advanced tools to identify and monitor users on an immense scale. As a result of these trends, global internet freedom declined for the ninth consecutive year in 2019.

Social media allow ordinary people, civic groups, and journalists to reach a vast audience at little or no cost, but they have also provided an extremely useful and inexpensive platform for malign influence operations by foreign and domestic actors alike. Political leaders employed individuals to surreptitiously shape online opinions in 38 of the 65 countries covered in this report—a new high. In many countries, the rise of populism and far-right extremism has coincided with the growth of hyperpartisan online mobs that include both authentic users and fraudulent or automated accounts. They build large audiences around similar interests, lace their political messaging with false or inflammatory content, and coordinate its dissemination across multiple platforms.

Cross-border influence operations, which first drew widespread attention as a result of Russian interference in the 2016 US presidential contest, are also an increasingly common problem. Authorities in China, Iran, Saudi Arabia, and a growing list of other countries have expanded their efforts to manipulate the online environment and influence foreign political outcomes over the past year. Malicious actors are no doubt emboldened by the failure of democratic states to update transparency and financing rules that are vital to free and fair elections, and apply them effectively to the online sphere.

While social media have at times served as a level playing field for civic discussion, they are now tilting dangerously toward illiberalism.

In addition to facilitating the dissemination of propaganda and disinformation during election periods, social media platforms have enabled the collection and analysis of vast amounts of data on entire populations. Sophisticated mass surveillance that was once feasible only for the world's leading intelligence agencies is now affordable for a much broader range of states. Freedom House research indicates that more repressive governments are acquiring social media surveillance tools that employ artificial intelligence to identify perceived threats and silence undesirable expression. Even in democracies, such mass monitoring is spreading across government agencies and being used for new purposes without adequate safeguards. The result is a sharp global increase in the abuse of civil liberties and shrinking online space for civic activism. Of the 65 countries assessed in this report, a record 47 featured arrests of users for political, social, or religious speech.

The future of internet freedom rests on our ability to fix social media.

While authoritarian powers like China and Russia have played an enormous role in dimming the prospects for technology to deliver greater human rights, the world's leading social media platforms are based in the United States, and their exploitation by antidemocratic forces is in large part a product of American neglect. Whether due to naïveté about the internet's role in democracy promotion or policymakers' laissez-faire attitude toward Silicon Valley, we now face a stark reality: the future of internet freedom rests on our ability to fix social media. This report offers a series of recommendations to that end, but whatever the specific solutions, the United States must take the lead in rallying defenders of the open internet to fairly regulate a technology that has become a necessity for our commerce, politics, and personal lives.

There is no more time to waste. Emerging technologies such as advanced biometrics, artificial intelligence, and fifth-generation mobile networks will provide new opportunities for human development, but they will also undoubtedly present a new array of human rights challenges. Strong protections for democratic freedoms are necessary to ensure that the internet does not become a Trojan horse for tyranny and oppression. The future of privacy, free expression, and democratic governance rests on the decisions we make today.

GLOBAL INTERNET USER STATS

Over **3.8 billion** people have access to the internet.

According to Freedom House estimates:

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

65% live in countries where individuals have been attacked or killed for their online activities since June 2018.

59% live in countries where authorities deployed progovernment commentators to manipulate online discussions.

56% live in countries where political, social, or religious content was blocked online.

46% live in countries where authorities disconnected internet or mobile networks, often for political reasons.

46% live in countries where access to social media platforms was temporarily or permanently restricted.

A man holds up a sign saying "Error 404 Demokratie not found" at a rally called "Save Your Internet," held shortly before the decisive vote on the reform of copyright and internet regulations in the EU Parliament. Opponents of the regulations held protests in about 20 countries. (Photo Credit: Sebastian Gollnow/picture alliance via Getty Images)

Tracking the Global Decline

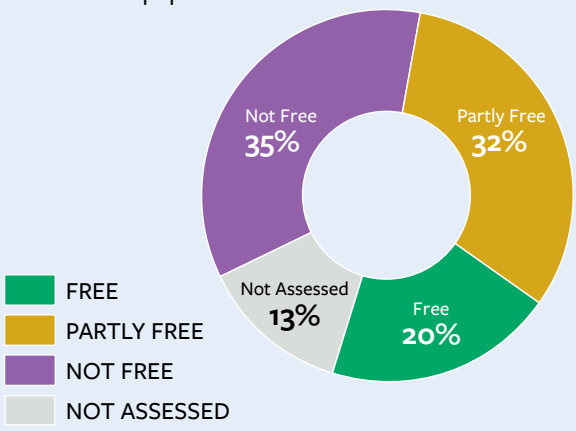
Freedom on the Net is a comprehensive study of internet freedom in 65 countries around the globe, covering 87 percent of the world's internet users. It tracks improvements and declines in internet freedom conditions each year. The countries included in the study have been selected to represent diverse geographical regions and regime types. In-depth reports on each country can be found at 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. Country-specific data underpinning this year's trends is available online. This report, the ninth in its series, focuses on developments that occurred between June 2018 and May 2019.

Of the 65 countries assessed, 33 have been on an overall decline since June 2018, compared with 16 that registered net improvements. The biggest score declines took place in Sudan and Kazakhstan followed by Brazil, Bangladesh, and Zimbabwe.

GLOBAL INTERNET POPULATION BY 2019 FOTN STATUS

Freedom on the Net assesses 87 percent of the world's internet user population.



In Sudan, nationwide protests sparked by devastating economic hardship led to the ouster of President Omar al-Bashir after three decades in power. Authorities blocked social media platforms on several occasions during the crisis, including a two-month outage, in a desperate and ultimately ineffective attempt to control information flows. The suspension of the constitution and the declaration of a state of emergency further undermined free expression in the country. Harassment and violence against journalists, activists, and ordinary users escalated, generating multiple allegations of torture and other abuse.

In Kazakhstan, the unexpected resignation of longtime president Nursultan Nazarbayev—and the sham vote that confirmed his chosen successor in office—brought simmering domestic discontent to a boil. The government temporarily disrupted internet connectivity, blocked over a dozen local and international news websites, and restricted access to social media platforms in a bid to silence activists and curb digital mobilization. Also contributing to the country's internet freedom decline were the government's efforts to monopolize the mobile market and implement real-time electronic surveillance.

The victory of Jair Bolsonaro in Brazil's October 2018 presidential election proved a watershed moment for digital election interference in the country. Unidentified actors mounted cyberattacks against journalists, government entities, and politically engaged users, even as social media manipulation reached new heights. Supporters of Bolsonaro and his far-right "Brazil over Everything, God above Everyone" coalition spread homophobic rumors, misleading news, and doctored images on YouTube and WhatsApp. Once in office, Bolsonaro hired communications consultants credited with spearheading the sophisticated disinformation campaign.

In Bangladesh, citizens organized mass protests calling for better road safety and other reforms, and a general election was marred by irregularities and violence. To maintain control over the population and limit the spread of unfavorable information, the government resorted to blocking independent news websites, restricting mobile networks, and arresting journalists and ordinary users alike.

Deteriorating economic conditions in Zimbabwe made the internet less affordable. As civil unrest spread throughout the country, triggering a violent crackdown by security forces, authorities restricted connectivity and blocked social media platforms.

China confirmed its status as the world's worst abuser of internet freedom for the fourth consecutive year. Censorship reached unprecedented extremes as the government enhanced its information controls in advance of the 30th anniversary of the Tiananmen Square massacre and in the face of widespread antigovernment protests in Hong Kong. In a relatively new tactic, administrators shuttered individual accounts on the hugely popular WeChat social media platform for any sort of "deviant" behavior, including minor infractions such as commenting on environmental disasters, which encouraged pervasive self-censorship. Officials have reported removing tens of thousands of accounts for allegedly "harmful" content on a quarterly basis. The campaign cut individuals off from a multifaceted tool that has become essential to everyday life in China, used for purposes ranging from transportation to banking. This blunt penalty has also narrowed avenues for digital mobilization and further silenced online activism.

Internet freedom declined in the United States. While the online environment remains vibrant, diverse, and free from state censorship, this report's coverage period saw the third straight year of decline. Law enforcement and immigration agencies expanded their surveillance of the public, eschewing oversight, transparency, and accountability mechanisms that might restrain their actions. Officials increasingly monitored social media platforms and conducted warrantless searches of travelers' electronic devices to glean information about constitutionally protected activities such as peaceful protests and critical reporting. Disinformation was again prevalent around major political events like the November 2018 midterm elections and congressional confirmation hearings for Supreme Court nominee Brett Kavanaugh. Both domestic and foreign actors manipulated content for political purposes, undermining the democratic process and stoking divisions in American society. In a positive development for privacy rights, the Supreme Court ruled that warrants are required for law enforcement agencies to access subscriber-location records from third parties.

Only 16 countries earned improvements in their internet freedom scores, and most gains were marginal. Ethiopia recorded the biggest improvement this year. The April 2018 appointment of Prime Minister Abiy Ahmed led to an ambitious reform agenda that loosened restrictions on the internet. Abiy's government unblocked 260 websites, including many known to report on critical political issues. Authorities also lifted a state of emergency imposed by the previous government, which eased legal restrictions on free expression, and reduced the number of people imprisoned for online activity. Although the government continued to impose network shutdowns, they were temporary and localized, unlike the nationwide shutdowns that had occurred in the past.

Other countries also benefited from an opening of the online environment following political transitions. A new coalition government in Malaysia made good on some of its democratic promises after winning May 2018 elections and ending the six-decade reign of the incumbent coalition. Local and international websites that were critical of the previous government were unblocked, while disinformation and the impact of paid commentators known as "cybertroopers" began to abate. However, these positive developments were threatened by a rise in harassment, notably against LGBT+ users and an independent news website, and by the 10-year prison term imposed on a user for Facebook comments that were deemed insulting to Islam and the prophet Muhammad.

In Armenia, positive changes unleashed by the 2018 Velvet Revolution continued, with reformist prime minister Nikol Pashinyan presiding over a reduction in restrictions on content and violations of users' rights. In particular, violence against online journalists declined, and the digital news media enjoyed greater freedom from economic and political pressures.

Iceland became the world's best protector of internet freedom, having registered no civil or criminal cases against users for online expression during the coverage period. The country boasts enviable conditions, including near-universal connectivity, limited restrictions on content, and strong protections for users' rights. However, a sophisticated nationwide phishing scheme challenged this free environment and its cybersecurity infrastructure in 2018.

Politicians and hyperpartisans use digital means to manipulate elections

Digital platforms are the new battleground for democracy. Shaping the flow of information on the internet is now an essential strategy of those seeking to disrupt the democratic transfer of power through elections. Incumbent political actors around the globe use both blunt and nuanced methods to deter opposition movements while preserving a veneer of popular legitimacy. Such internet freedom restrictions tend to escalate before and during crucial votes.

Major authoritarian powers like Russia and China have been implicated in cyberattacks and information warfare linked to elections in democratic states. In February 2019, three months before Australia's federal elections, security agencies reported a cyberattack against the computer networks of Parliament and the three main political parties that was attributed to China's Ministry of State Security. Ukraine's Central Election Commission faced a wave of cyberattacks, likely emanating from Russia, ahead of the April–May 2019 presidential election. In the run-up to the November 2018 midterm elections in the United States, Microsoft discovered that a unit associated with Russian military intelligence had created websites resembling those of the US Senate and prominent Republican-linked think tanks, in a bid to trick visitors into revealing sensitive information and passwords. Groups associated with Russia also spread disinformation across Twitter, Facebook, and YouTube during the May 2019 European Parliament elections. Such cross-border interference is meant to sow division, support favored candidates, and undermine democracy.

> Populists and far-right leaders have grown adept not only at creating viral disinformation, but also at harnessing networks that disseminate it.

In a majority of countries evaluated, however, it was domestic actors who abused information technology to subvert the electoral process. In the 30 countries that held elections or referendums during the coverage period, Freedom House found three distinct forms of digital election interference: informational measures, in which online discussions are surreptitiously manipulated in favor of the government or particular parties; technical measures, which are used to restrict access to news sources, communication tools, and in some cases the entire internet; and legal measures, which authorities apply to punish regime opponents and chill political expression.

The prevalence of the three digital interference tactics varied across the democratic spectrum. Most strikingly, countries labeled Partly Free by *Freedom in the World,* an annual Freedom House report that assesses political rights and civil liberties, were most likely to suffer internet freedom score declines surrounding elections. This may reflect the fact that elections in such countries remain somewhat competitive, meaning incumbents with authoritarian ambitions find it necessary to intensify censorship and manipulation in order to remain in power.

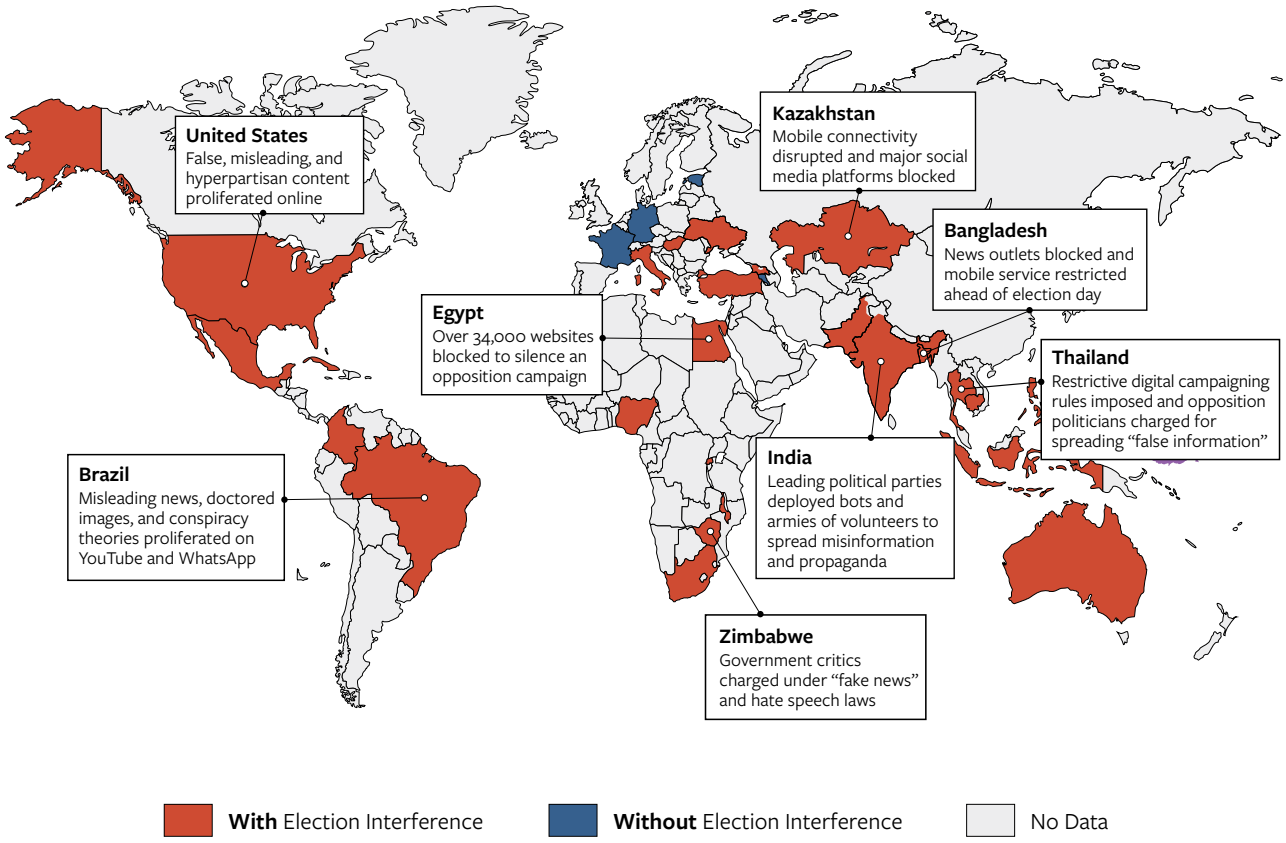
Informational measures: Manipulating content with new sophistication

State and nonstate actors employed informational measures to distort the media landscape during elections in 24 countries over the past year, making it by far the most popular tactic. Freedom House previously outlined five major methods of content manipulation: propagandistic news, outright fake news, paid commentators, bots (automated accounts), and the hijacking of real social media accounts.

This year, populists and far-right leaders have grown adept not only at creating viral disinformation, but also at harnessing networks that disseminate it. Some such networks are explicitly directed by state or party officials, while others are semiautonomous, lending support to their political champions and receiving encouragement and approval in return. Working in tandem with government-friendly

THE GLOBAL PHENOMENON OF DIGITAL ELECTION INTERFERENCE

Domestic actors interfered online in 26 of 30 countries that held elections or referendums over the past year.



media personalities and business magnates, these online mobs amplify conspiracy theories, inflammatory views, and misleading memes from small echo chambers to the political mainstream.

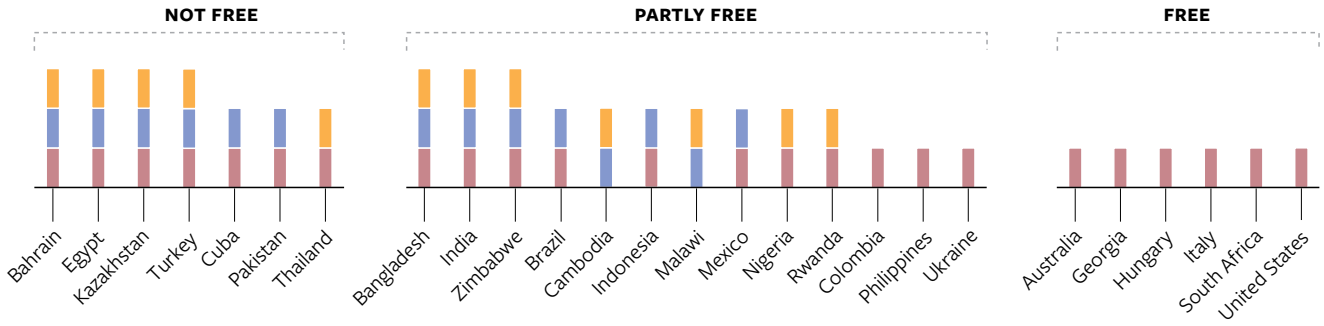
In several countries that held elections, extremist parties seemed better equipped to exploit social media than their moderate rivals. Far-right groups may enjoy more success because—as studies have shown—false, shocking, negative, exaggerated, and emotionally charged content tends to spread faster and wider on social media platforms than other types of content. Moreover, the electoral authorities in most countries have yet to build sufficient oversight mechanisms for identifying and thwarting this type of electoral interference. The risk of punishment for skirting the relevant rules generally pales in comparison with the gains of winning an election.

In advance of Brazil's October 2018 elections, the electoral court convened a special advisory council to better enforce strict rules on campaigning. Candidates and media outlets signed a pact to refrain from sharing fake news. Despite these efforts, political disinformation rose to a new level of intensity. Jair Bolsonaro and his far-right movement amassed a large following by spouting conspiracy theories on YouTube and taking advantage of the platform's propensity to steer viewers toward ever-more radical videos. Operatives

The risk of punishment for skirting election rules generally pales in comparison with the gains of winning.

KEY TACTICS OF DIGITAL ELECTION INTERFERENCE

Freedom House identified three distinct forms of domestic digital interference. Strikingly, informational tactics were by far the most popular.



Informational tactics

The coordinated use of hyperpartisan commentators, bots, group admins, or news sites to disseminate false or misleading content, often with the backing of the state or a political party apparatus.

Technical tactics

Intentional restrictions on connectivity; blocking of social media platforms and websites; and cyberattacks from suspected domestic actors on political websites or social media accounts.

Legal tactics

Arrests of individuals for online political expression, as well as the establishment of new laws and regulations that criminalize online speech.

employed special software to scrape phone numbers from Facebook and automatically add recipients to a network of coordinated WhatsApp groups, based on identifiers like location, gender, or income level. Some of these echo chambers averaged more than 1,000 posts per day, with group administrators pumping out misleading memes on Bolsonaro's main opponent and mobilizing supporters to harass critics. Local business groups reportedly funded an additional WhatsApp disinformation campaign against Bolsonaro's opponent, in an apparent violation of campaign finance rules.

Mainstream political parties in India undertook similar strategies during general elections in April and May 2019. The ruling Bharatiya Janata Party (BJP) and the opposition Indian National Congress respectively deployed 1.2 million and 800,000 die-hard supporters to create and disseminate disinformation that amplified the party line on platforms including WhatsApp and Facebook. In addition, millions of users were flooded with misleading and inflammatory content on Prime Minister Narendra Modi's "NaMo" app, which had been marketed to all Indians as a way to keep up with official government news; top officials in India's National Cadet Corps, an all-volunteer youth wing of the Indian military, encouraged its 1.3 million cadets to download the app, which is privately owned by Modi and operated by the BJP. A researcher revealed that the app was secretly routing users' personal information to a behavioral analytics company with offices in the United States and India.

Candidates in the Philippines, where disinformation tactics were pioneered during elections in 2016, updated their manipulation strategies for the May 2019 polls. To circumvent technology companies' efforts to limit false and misleading news, political operatives spread information through closed groups on public platforms, where there is less content moderation, as well as through hyperpartisan alternative news channels on YouTube and Facebook. In another new tactic, candidates paid social media personalities with small- to medium-sized followings to promote their campaigns on Facebook, Twitter, and Instagram. The "micro-influencers" sprinkled political endorsements among sexually suggestive images and pop-culture news. Compared with advertising on more popular accounts, these sponsored posts cost less money and appear more authentic, and they are not labeled as advertisements, allowing for the skirting of spending limits. In these conditions, the Philippines' disinformation market has blossomed. Public relations and advertising professionals sell their services for as much as 30 million pesos ($580,000) for a three-month campaign.

Despite civil society's early efforts to expose domestic disinformation in many countries, the campaigns are only growing in reach. Informational measures to interfere in elections may not carry the same stigma as technical and legal measures, though that is something the international community and civil society can work to change. Authoritarians are keenly aware of the "costs" of arresting prominent opposition members, for example, but in bots and trolls they have found ways to manipulate the media while maintaining plausible deniability on their own involvement.

Technical measures: Blocking, hacking, and cutting off access

Technical measures played a role in the elections of at least 14 countries during the coverage period. Most commonly, officials targeted specific websites that they considered a threat to the rule of incumbent leaders. For example in Egypt, where political, press, and internet freedoms have all been eviscerated, citizens nevertheless launched an online campaign to voice opposition to proposed constitutional amendments that were designed to expand the extraordinary power of the military, extend the president's control over the judiciary, and open the door for President Abdel Fattah al-Sisi to remain in office through 2030. The #Batel, or #Void, campaign gathered 60,000 signatures on its first day before being blocked. As campaigners published multiple mirrors, or copies, of the website on different URLs, those too were blocked, and at least 34,000 websites were rendered inaccessible as collateral damage. In the absence of any real debate, the amendments were adopted by a reported 89 percent of voters in a deeply flawed April 2019 referendum.

On the evening before and the day of Cambodia's July 2018 general elections, the Information Ministry ordered service providers to temporarily block over a dozen independent news outlets, including Radio Free Asia, Voice of America, and the *Phnom Penh Post*. The government, led for the past three decades by authoritarian prime minister Hun Sen, justified the move by citing a legal prohibition on campaigning within 24 hours of voting, even though the outlets were merely providing crucial information for voters to make informed choices at the ballot box. Authorities did not block scores of news outlets that were perceived to be less critical of the government. In the final result, the ruling Cambodian People's Party won every seat in the lower house of Parliament, as the main opposition party had been formally banned in 2017.

In July 2018, Zimbabwe held its first election since the military's November 2017 ouster of President Robert Mugabe, who had controlled the ruling Zimbabwe African National Union–Patriotic Front (ZANU-PF) since the country's independence in 1980. Following the vote, the website of a British-based advocacy organization, Zimelection.com, was blocked by the state-owned telecommunications firm TelOne, though it remained accessible via privately owned service providers. The discrepancy illustrated how state ownership of the telecommunications infrastructure can facilitate indirect or ad hoc blocking of resources deemed to be critical of the government. The opposition ultimately lost the vote, with ZANU-PF and its new leader, President Emmerson Mnangagwa, maintaining their grip on power.

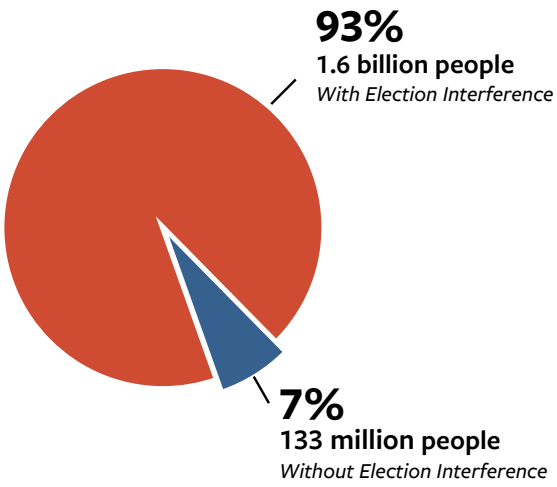
> Governments restricted access to specific apps and platforms used by the opposition to mobilize, or resorted to shutting down the internet altogether.

In several other countries, governments restricted access to specific apps and platforms used by the opposition to mobilize, or resorted to shutting down the internet altogether. In Bangladesh, authorities briefly blocked Skype after noticing that it was used by exiled opposition leaders to communicate with local activists. Officials quickly determined that measure was insufficient; they repeatedly restricted mobile internet service throughout the country prior to and on election day in December 2018, preventing all Bangladeshis from using any messaging or social media applications on their mobile devices. The ruling Awami League and its allies won the elections in a landslide, securing all but 12 of the 300 parliament seats up for grabs. During the coverage period, some citizens in India, Kazakhstan, Malawi, and Pakistan were also denied internet connectivity around voting in their countries.

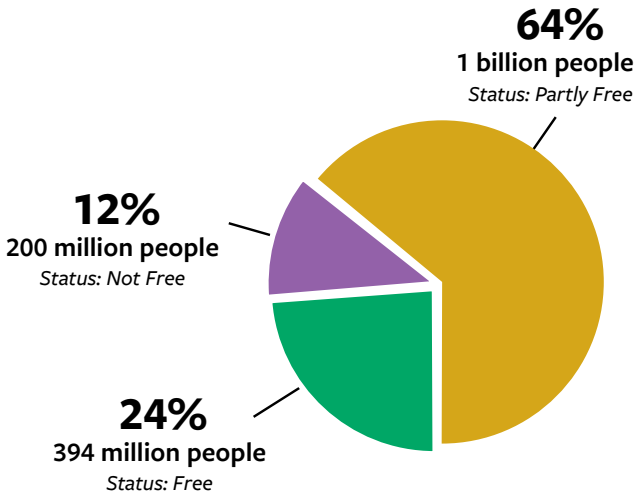
Technical restrictions often take the form of cyberattacks. Ahead of the July 2018 presidential election in Mexico, a distributed denial-of-service (DDoS) attack brought down the website of the opposition National Action Party on the same day that documents critical of eventual winner Andrés Manuel López Obrador were published. In Brazil, a journalist who alleged campaign violations by Jair Bolsonaro had her account hacked, with the perpetrators sending pro-Bolsonaro messages to her contacts. The website of a fact-checking project, Cekfakta, was hacked in Indonesia shortly after a live debate of presidential candidates.

WHO IS AFFECTED BY ELECTION INTERFERENCE?

In countries that held elections or referendums, an alarming number of internet users were exposed to informational, technical, or legal interference by domestic actors.



Internet users living in countries ranked Partly Free were most likely to experience election interference.



Legal measures: Passing new restrictions and punishing dissent

In 12 countries, authorities employed legal measures, such as criminal charges, to control online speech during election periods. One of the most common charges was defaming public officials. For example, authorities in Malawi arrested two social media activists for posts that were deemed insulting to the president and first lady in the months leading up to May 2019 elections. In Turkey, police arrested several individuals for insulting President Recep Tayyip Erdoğan on social media ahead of presidential and parliamentary elections in June 2018. Prior to India's elections, police detained a journalist under the National Security Act for criticizing the BJP and Prime Minister Modi on Facebook, and the social media chief of the opposition Indian National Congress faced sedition charges for sharing a meme calling Modi a thief.

When existing legal measures seemed insufficient, incumbents introduced new rules or legislation to help control the online environment. A few months before Bangladesh's general elections, Prime Minister Sheikh Hasina's government passed a law prescribing prison sentences for certain types of online "propaganda." This so-called Digital Security Act was subsequently used to arrest the editor of Daily71.com, a news outlet, for failing to toe the government's line. Similarly, the Election Commission of Thailand issued vague and restrictive rules regulating what type of content parties and candidates could share on social media, and imposed criminal liability for noncompliance. One candidate for the opposition Pheu Thai Party chose to self-censor and deactivate her Facebook account to avoid violating the commission's rules. Although opposition parties collectively won the most votes in the March 2019 elections, the first to be held since a 2014 military coup, the head of the junta stayed on as prime minister thanks to antidemocratic provisions in the new, military-backed constitution.

The fight to preserve the internet as a tool for democratic progress

Elections are a flashpoint for online censorship around the world because most leaders with authoritarian ambitions continue to rely on votes to maintain the appearance of legitimacy, and they recognize that the internet remains a potent instrument for challenging state power and asserting fundamental freedoms.

In Russia, after more than 50 opposition candidates were barred from running in Moscow's city council elections in September 2019, protests erupted and spread across the country for nearly two months. The protesters used innovative digital communications tools to coordinate their activities, which included medical support, legal assistance for those detained, delivery of food and other aid packages, and providing money to cover administrative fines. Moreover, many citizens used a website and app that helped them identify and vote for candidates most likely to defeat those of the ruling party. Progovernment candidates suffered a surprising setback in the eventual Moscow vote.

Developments in Armenia in 2018 demonstrated once again that digital technology can help generate dramatic democratic change. Citizens effectively used social media platforms, communications apps, and live streaming to advance the largely peaceful Velvet Revolution, forcing the resignation of longtime leader Serzh Sargsyan and ushering in Nikol Pashinyan as prime minister. This in turn cleared the way for snap national elections in December 2018 that represented a clear improvement over previous polls. The new government has since promised to tackle systemic corruption and enhance transparency and the rule of law.

A pivotal struggle to defend and advance basic democratic rights is still unfolding in Hong Kong, where protesters began turning out in June 2019 to oppose a controversial extradition bill and demand a rollback of Beijing's encroachment on their legal and political rights. Acutely aware of government surveillance, protesters used various techniques to avoid online detection and reprisals, including code words like "picnic" to signify a meeting. After reports emerged that authorities might shut off the internet, demonstrators tested peer-to-peer or mesh networks that send messages through Bluetooth wireless technology instead of relying on full connectivity.

> The internet remains a potent instrument for challenging state power and asserting fundamental freedoms.

Even in countries where democratic institutions are fairly robust, citizens increasingly rely on digital technologies to participate in political affairs and engage in urgent policy debates. Social media in democracies are used to mobilize public support on a host of issues, such as minority rights, environmental protection, safer gun laws, and improved health care. The onus is on policymakers, the private sector, and civil society to make sure that these positive uses of the internet are protected—at home and abroad—from the forms of malicious interference described above. This will mean years of work to establish clear rules, build tools, and develop programs that meaningfully respond to the grave and growing threat such manipulation poses to the democratic process.

A protester holds an illuminated cellphone while forming a human chain during the Hong Kong Way anti-government rally across Kowloon in Hong Kong. (Photo Credit: Miguel Candela/SOPA Images/LightRocket via Getty Images)

Governments harness big data for social media surveillance

Governments are increasingly purchasing sophisticated technology to monitor their citizens' behavior on social media. Once the preserve of the world's foremost intelligence agencies, this form of mass surveillance has made its way to a range of countries, from major authoritarian powers to smaller or poorer states that nevertheless hope to track dissidents and persecuted minorities. The booming commercial market for social media surveillance has lowered the cost of entry not only for the security services of dictatorships, but also for national and local law enforcement agencies in democracies, where it is being used with little oversight or accountability. Coupled with an alarming rise in the number of countries where social media users have been arrested for their legitimate online activities, the growing employment of social media surveillance threatens to squeeze the space for civic activism on digital platforms.

> The growing use of social media surveillance threatens to squeeze the space for civic activism on digital platforms.

A shift to machine-driven monitoring of the public

Social media surveillance refers to the collection and processing of personal data pulled from digital communication platforms, often through automated technology that allows for real-time aggregation, organization, and analysis of large amounts of metadata and content. Broader in scope than spyware, which intercepts communications by targeting specific individuals' devices, social media surveillance cannot be dismissed as less invasive. Billions of people around the world use these digital platforms to communicate with loved ones, connect with friends and associates, and express their political, social, and religious beliefs. Even when it concerns individuals who seldom interact with such services, the information that is collected, generated, and inferred about them holds tremendous value not only for advertisers, but increasingly for law enforcement and intelligence agencies as well.

Governments have long employed people to monitor speech on social media, including by creating fraudulent accounts to connect with real-life users and gain access to networks. Authorities in Iran have boasted of a 42,000-strong army of volunteers who monitor online speech. Any citizen can report for duty on the Cyber Police (FATA) website. Similarly, the ruling Communist Party in China has recruited thousands of individuals to sift through the internet and report problematic content and accounts to authorities.

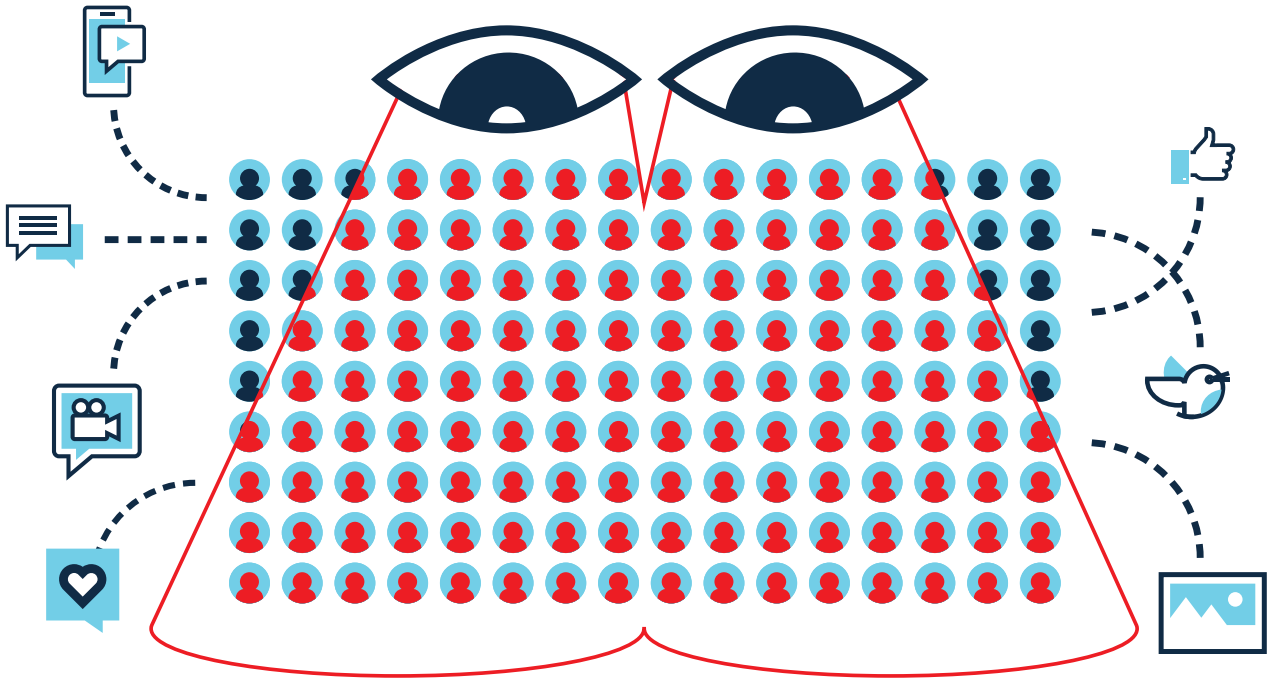
Advances in artificial intelligence (AI) have opened up new possibilities for automated mass surveillance. Sophisticated monitoring systems can quickly map users' relationships through link analysis; assign a meaning or attitude to their social media posts using natural-language processing and sentiment analysis; and infer their past, present, or future locations. Machine learning enables these systems to find patterns that may be invisible to humans, while deep neural networks can identify and suggest whole new categories of patterns for further investigation. Whether accurate or inaccurate, the conclusions made about an individual can have serious repercussions, particularly in countries where one's political views, social interactions, sexual orientation, or religious faith can lead to closer scrutiny and outright punishment.

The global market for surveillance

The market for social media surveillance has grown, giving intelligence and law enforcement agencies new tools for combing through massive amounts of information. At least 40 of the 65 countries covered by this report have instituted advanced social media monitoring programs. Moreover, their use by governments is accelerating: in 15 of these countries, it was only in the past year that such programs were either expanded or newly established. Justifying their efforts in the name of enhancing security, limiting disinformation, and ensuring public order, governments have effectively co-opted social media platforms. While these platforms typically

UNDER THE WATCHFUL EYE OF SOCIAL MEDIA SURVEILLANCE

40 of the 65 countries covered by *Freedom on the Net* have instituted advanced social media surveillance programs. That means 89% of internet users—or nearly 3 billion people—are being monitored.



present themselves as social connectors and community builders, state agencies in repressive countries see them as vast storehouses of speech and personal information that can be observed, collected, and analyzed to detect and suppress dissent.

China is a leader in developing, employing, and exporting social media surveillance tools. The Chinese firm Semptian has touted its Aegis surveillance system as providing "a full view to the virtual world" with the capacity to "store and analyze unlimited data." The company claims to be monitoring over 200 million individuals in China—a quarter of the country's internet users. The company even markets a "national firewall" product, mimicking the so-called Great Firewall that controls internet traffic in China.

Chinese agencies work closely with leading companies to monitor individuals online. A security researcher discovered an unsecured database consisting of the social media profiles, messages, and shared files of some 364 million Chinese users, updated daily, for manual tracking by law enforcement. A complex web of regulations gives the Chinese state access to user content and metadata, allowing authorities to more easily identify and reprimand users who share sensitive content. In March 2019, for example, it was reported that a member of Xinjiang's persecuted Uighur Muslim minority population was detained and interrogated for three days because someone on his WeChat contact list had "checked in" from Mecca, Saudi Arabia.

China is a leader in developing, employing, and exporting social media surveillance tools.

FREEDOM ON THE NET 2019

Status	Countries
FREE	15
PARTLY FREE	29
NOT FREE	21
Total	**65**

For more information about the report's geographical coverage, visit freedomonthenet.org.

A police officer monitors various social media channels at the Punjab Police Integrated Command, Control and Communication Center (IC3) in Lahore, Pakistan. (Photo Credit: Asad Zaidi/Bloomberg via Getty Images)

Further, several provincial governments in China are reportedly developing a "Police Cloud" system to aggregate data from users' social media accounts, telecoms records, and e-commerce activity, as well as biometric data and video surveillance footage. The big data policing system can target individuals for interacting with "persons of concern" or for belonging to "certain ethnicities," a euphemism applying to the Uighur Muslim minority. There, authorities have developed a host of invasive tools, both low- and high-tech, for repressing any behavior that strays from what is acceptable under Xi Jinping Thought—the doctrine of China's authoritarian leader.

Of the 15 countries in Asia assessed by this report, 13 have social media surveillance programs under development or in use. In Vietnam, the Communist Party government in October 2018 announced a new national surveillance unit equipped with technology to analyze, evaluate, and categorize millions of social media posts. The government has long punished nonviolent activists for what they write on social media; weeks before the October announcement, human rights defender and environmentalist Lê Đình Lượng was convicted and sentenced to 20 years in prison after a one-day trial for trying to overthrow the state, in part for Facebook posts criticizing the government. The new technology will likely enable the government to intensify its crackdown. Meanwhile, Pakistan in February 2019 announced a new social media monitoring program meant to combat extremism, hate speech, and antinational content. Only a month later, the Interior Ministry launched an investigation into journalists and activists who had expressed support for murdered Saudi journalist Jamal Khashoggi on their social media accounts.

Some countries in Asia are developing their social media surveillance capabilities in close cooperation with US authorities. In September 2018, Philippine officials traveled to North Carolina for training by US Army personnel on developing a new social media monitoring unit. While authorities claim the unit is intended to combat disinformation by violent extremist organizations, the Philippine government's broad labeling of critical journalists and users as terrorists suggests that monitoring efforts will extend far beyond any legitimate security threat. Bangladesh's Rapid Action Battalion (RAB) was approved to travel to the United States in April 2019 to receive training on "Location Based Social Network Monitoring System Software." The RAB, which is infamous for human rights violations including extrajudicial killings, enforced disappearances, and torture, was given 1.2 billion taka ($14 million) by the Bangladeshi government for "state-of-the-art equipment" to monitor in real time what it considers to be rumors and propaganda. These developments occurred in a year when authorities led a violent crackdown on dissent during national protests and general elections.

The Middle East and North Africa region, home to some of the world's most repressive regimes, is also a booming market for social media surveillance. Companies scheduled to attend a Dubai trade show in 2020 represent countries including China, India, Israel, Italy, the United States, and the United Kingdom. Knowlesys, a Chinese company whose clients reportedly include the Chinese military and government bodies, will hold live demonstrations on how to "monitor your targets' messages, profiles, locations, behaviors, relationships, and more," and how to "monitor public opinion for election." Semptian, which has clients in the region, has a price range of $1.5 million to $2.5 million for monitoring the online activities of a population of five million people—an affordable price for most dictators.

In December 2018, it was reported that Kazakhstan had purchased a $4.3 million automated monitoring tool to track signs of political discontent on social media. The firm supplying the software is linked to Russia's Federal Security Service and has been subjected to sanctions by the US Treasury Department for its activities surrounding the 2016 US elections. Screenshots revealed that the product uses deep learning to "detect materials that discredit the state." The tools could easily be abused in Kazakhstan, where individuals have received multiyear prison sentences for social media posts that are deemed supportive of the Democratic Choice of Kazakhstan, a banned opposition party.

Russia has used sophisticated social media surveillance tools for many years. The government issued three tenders in 2012 for the development of research methods related to "social networks intelligence," "tacit control on the internet," and "a special software package for the automated dissemination of information in large social networks," foreshadowing how intelligence agencies would eventually master the manipulation of social media at home and abroad. This May, authorities released a tender for technology to collect, analyze, and conduct sentiment analysis on social media content relating to President Vladimir Putin and other topics of interest to the government. The year featured more protest-related arrests, internet shutdowns, and legal restrictions in Russia, suggesting that any new monitoring technology would simply add to the government's arsenal of tools for clamping down on unauthorized political mobilization.

> The expanding use of sophisticated social media surveillance tools raises the risk that constitutionally protected activities will be impaired.

Monitoring projects are under way in Africa as well. The government of Nigeria allocated 2.2 billion naira ($6.6 million) in its 2018 budget for a "Social Media Mining Suite," having already ordered the military to watch for antigovernment content online. In an ominous sign, the country experienced an increase in arrests for internet activity over the past year. Human rights and democracy activist Ibrahim Garba Wala, known as IG Wala, was sentenced in April to 12 years in prison for criminal defamation, public incitement, and unlawful assembly; the charges stemmed from Facebook posts alleging corruption in the National Hajj Commission. Israeli firms Verint and WebIntPro have reportedly sold similar surveillance software to Angola and Kenya, respectively.

In strong democracies, new tools of potential repression

The social media surveillance tools that have appeared in democracies got their start on foreign battlefields and in counterterrorism settings, designed to monitor acute security threats in places like Syria. Many US data-mining companies received seed money from the Central Intelligence Agency through its In-Q-Tel venture capital fund. While authorities

in the past typically justified the use of these tools with the need to combat serious crimes such as terrorism, child sexual abuse, and large-scale narcotics trafficking, law enforcement and other agencies at the local, state, and federal levels are increasingly repurposing them for more questionable practices, such as screening travelers for their political views, tracking students' behavior, or monitoring activists and protesters. This expansion makes oversight of surveillance policies more difficult and raises the risk that constitutionally protected activities will be impaired.

For example, in the United States, agencies within the Department of Homeland Security (DHS)—including Customs and Border Protection (CBP), Citizenship and Immigration Services, and Immigration and Customs Enforcement (ICE)—have used automated technology to collect and analyze personal information, with limited oversight and transparency. By claiming that its power to conduct warrantless searches extends within a 100-mile radius of any US border, DHS has effectively asserted extrajudicial surveillance powers over 200 million people. CBP has even purchased technology from Cellebrite, an Israeli company, to bypass encryption and passwords and enable quick extraction of data from phones and computers, including social media content. There has been a spike in device searches at the borders in recent years; the number of such searches, normally limited under the Fourth Amendment of the constitution, increased by 292 percent, from 8,503 to 33,295, between fiscal year 2015 and fiscal year 2018. Over that same period, inbound travel to the United States increased by less than 3 percent.

> Authorities in 47 countries arrested users for political, social, or religious speech—a record high.

These searches have become part of the government's drive toward big data surveillance. The resulting information is frequently deposited in massive multiagency databases where it can be combined with public records, secret intelligence materials, and datasets (including social media data) assembled by private companies. In one case, ICE paid the data analytics company Palantir $42.3 million for a one-year contract related to FALCON, a custom-built database management tool. Its "Search and Analysis System" enables agents to analyze trends and establish links between individuals based on information gathered during border searches, purchased from private data brokers, and obtained from other intelligence collection exercises. Similar tools developed by Palantir are used by some 300 police departments in the state of California alone, as well as by police forces in Chicago, Los Angeles, New Orleans, and New York City. Many of these programs are facilitated through DHS and its Regional Intelligence Centers.

The consequences of government intrusion into the digital public square

For authoritarian and democratic governments alike, the potential for abuse presented by advanced social media surveillance is staggering. In 2019, Freedom House found that 47 of the 65 countries assessed featured arrests of users for political, social, or religious speech—a record high. The blanket monitoring of online activities for undesirable or illegal speech will undoubtedly lead to more arrests, particularly in environments that lack strong protections for free expression. Monitoring designed to detect and deter protests will also help stifle democracy movements in authoritarian settings.

Even in countries with considerable safeguards for fundamental freedoms, there are already reports of abuse. In the United Kingdom, for example, London police reportedly monitored nearly 9,000 activists from across the political spectrum—many of whom had no criminal background—using geolocation tracking and sentiment analysis on data scraped from Facebook, Twitter, and other platforms. This information was then compiled in secret dossiers on each campaigner. Similar dynamics are evident in the United States, where leaked documents revealed in March 2019 that CBP had created a list of 59 US and foreign immigration activists, journalists, lawyers, and Facebook group administrators who should be targeted for greater scrutiny at the US-Mexico border, leading to arrests in nine cases. ICE has also monitored social media in New York City to gather information on groups protesting the administration's immigration and gun-control policies. Such profiling poses a distinct threat to basic civil liberties. As the US Supreme Court ruled in 1958, "inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."

SOCIAL MEDIA SURVEILLANCE ERODES RIGHTS

Authorities can collect and analyze details about personal relationships, spiritual beliefs, and sexual preferences, and share them with third parties.

Human and algorithmic bias perpetuates harmful and incorrect stereotypes, disproportionately impacting marginalized communities.

Immigration officials can deny individuals entry based on their political, social, or religious views expressed on social media, or that of their friends and family.

People refrain from speaking out on political, social, and religious issues when they fear their speech could be recorded and potentially used against them.

Individuals become less likely to join organizations and groups if authorities can monitor their memberships and activities.

Authorities can disrupt nonviolent demonstrations before they begin, and track the names of individuals in attendance.

Monitoring eschews democratic legal standards of "reasonable suspicion" and "probable cause," and instead treats everyone as a suspect of wrongdoing.

The chilling effect on free expression caused by increased surveillance is well documented. Activists and journalists who might otherwise hold governments to account for wrongdoing are more inclined to self-censor, while dissidents and members of marginalized communities will think twice about discussing their political opinions online to avoid arrests or travel restrictions. Furthermore, social media monitoring designed to quell mobilization and identify protesters hinders the public's ability to use online tools to associate and assemble peacefully. Finally, indiscriminate monitoring of the general population's online communications—even when those communications are nominally public—runs afoul of due process standards enshrined in democratic constitutions and international human rights law.

Protecting human rights in the age of AI surveillance

There is little if any public evidence that such technology is more effective than less-invasive alternatives for ensuring national security and combating serious crimes. Social media activity such as original content, likes, or shares—particularly speech that is rendered in slang or languages other than English—is susceptible to misinterpretation and misclassification. Research has estimated the accuracy rates of natural-language processing tools at 70 to 80 percent. While they are often justified as a means to reduce human error, algorithmic tools can further entrench racial or religious discrimination due to reliance on inaccurate or biased data. The resulting false positives can add innocent people to government watch lists, often without their knowledge, leaving them with little recourse for remedying the mistake.

Thanks to the development of AI-assisted tools, governments now have a greater capacity for surveillance than ever before.

At the very least, social media surveillance must come under greater oversight. The use of such programs must be transparent, including sustained dialogue between law enforcement and affected communities. Public civil rights assessments should be conducted, and authorities should be held accountable when tools are misused and offer remedies for any victims. Online surveillance technology should not be used to proactively monitor the planning and organization of peaceful protest activities or individuals' involvement in nonviolent political groups. And governments should swiftly amend existing privacy legislation to address the proper use of this technology.

Thanks to the development of AI-assisted tools, governments now have a greater capacity for surveillance than ever before. Given their potential impact on fundamental rights, policymakers and citizens must ask themselves whether these new tools are necessary or desirable in a democratic society. It is time to move beyond outdated arguments that individuals "should have nothing to hide" or do not have a reasonable expectation of privacy in public areas. The survival of democracy requires vibrant public spaces, both offline and online, where individuals can collaborate, organize, and go about their personal lives without fear of constant surveillance.

Recommendations

SECURING ELECTIONS

For Policymakers

- **Improve transparency and oversight of online political advertisements.** In the United States, the Honest Ads Act (S.1356/H.R.2592) would modernize existing law by applying disclosure requirements to campaign advertising and requiring large digital platforms to maintain a public file of all electioneering communications that includes a copy of each ad, when it was published, its target audience, the number of views generated, and the contact information of the purchaser. The Honest Ads Act would also require platforms that distribute political ads to make "reasonable efforts" to ensure that they are not being purchased by foreign actors, directly or indirectly.
- **Address the use of bots in social media manipulation.** In the United States, the Bot Disclosure and Accountability Act (S.2125) would authorize the Federal Trade Commission to require the conspicuous and public disclosure of bots intended to replicate human activity. The legislation would also prohibit candidates, campaigns, and political organizations from using such bots, particularly to disguise political advertising or otherwise deceive voters by giving false impressions of support from actual users.
- **Protect elections from cyberattacks with paper ballots and election audits.** According to the recommendations of the bipartisan report on Russian interference in the 2016 election released by the US Senate Select Committee on Intelligence, paper ballots ensure votes have a verifiable paper trail, while risk-limiting audits help ensure the accuracy of results. In the United States, the Protecting American Votes and Election Act (S.1472/H.R.2754) would mandate the use of paper ballots and audits in federal elections, and provide funding for states to purchase new ballot-scanning machines.

For the Private Sector

- **Develop rapid response teams to address cybersecurity and disinformation incidents around elections.** Ahead of significant elections and referendums in countries around the world, social media companies and other content providers should create specialized teams that anticipate digital interference, and devise strategies to prevent interference tactics and mitigate their effects. When designing and implementing new tools to address cybersecurity and disinformation, companies should communicate openly about what new policies they may be putting in place ahead of elections, and engage with local civil society organizations that can provide expertise on the political and cultural contexts in which companies work.
- **Ensure political advertisements are transparent and adhere to strict content standards.** Companies should rigorously vet political advertisements before they are posted on their platforms to ensure legitimate association with domestic actors and compliance with applicable electoral laws. Companies should also clearly identify who has purchased each advertisement.
- **Improve information sharing among social media companies and between public and private sectors.** As recommended by the US Senate Select Committee on Intelligence in its bipartisan report on Russia's use of social media to interfere in the 2016 US election, social media companies should improve and formalize mechanisms that allow them to share information about malicious activity and potential vulnerabilities on their platforms amongst themselves and with governments. This will allow faster and more effective responses to foreign disinformation campaigns and other forms of interference, which often span multiple platforms. Social media users should be notified when they may have been exposed to such foreign activity, and be given information necessary to understand the malicious nature of the content.

For Civil Society

- **Conduct early-warning analysis on election interference tactics likely to occur in a country, and mobilize advocacy campaigns to prevent negative impacts**. Civil society organizations (CSOs) should educate voters about how to spot political disinformation and flag misleading content on social media, particularly on private messaging platforms. Advocacy efforts should place public pressure on governments and telecommunications providers to refrain from blocking online content or restricting network connectivity. CSOs should also engage with election commissions to flag potential interference tactics and develop strategies to mitigate other harms to the electoral process.

PREVENTING ABUSIVE SOCIAL MEDIA SURVEILLANCE

For Policymakers

- **Strictly regulate the use of social media surveillance tools and the collection of social media information by government agencies and law enforcement.** To maintain democratic standards, any social media surveillance program employed by government or law enforcement must occur under stringent oversight and operate with transparency, including through sustained dialogue with local communities. Social media surveillance should not be used to proactively monitor peaceful protests or individuals' involvement in nonviolent political groups. Government agencies should not conduct blanket collection of social media data as part of immigration or visa evaluations. Given the technical limitations and known inaccuracy rates of such technology, relevant oversight agencies should conduct human rights audits of the tools themselves and their use, and release their results to the public. They should further be empowered to impose penalties, and require that those harmed be granted remedy.
- **Enact robust data privacy legislation.** In the United States, policymakers should pass a federal electronic privacy law that provides robust data protections and harmonizes rules among the 50 states. Individuals should have control over their information and the right to access it, delete it, and transfer it to the providers of their choosing. Companies should be required to disclose in nontechnical language how they use customer data, details of third parties that have access to the data, and how third parties use the data. Companies should also notify customers in a timely fashion if their data is compromised. Governments should have the ability to access personal data only in limited circumstances as prescribed by law and subject to judicial authorization, and only within a specific time frame. Given the technical measures—including cyber attacks—that both foreign and domestic actors use to access citizens' personal information, data privacy legislation should also be paired with cybersecurity requirements on the collection and amassing of user data.
- **Restrict the export of sophisticated monitoring tools.** Although established democracies also abuse social media surveillance technologies, authoritarian governments are more likely to do so. The United States is currently undergoing an interagency rulemaking process to determine which emerging dual-use technologies (those used by both civilians and militaries) should be subject to export controls. Any final rule issued by the US government should ensure that technologies enabling monitoring, surveillance, and the interception or collection of information and communications—including ones that use machine learning, natural language processing, and deep learning—are included on the Commerce Control List and their sale restricted from countries rated Partly Free or Not Free by any Freedom House publication. Further, democratic policymakers should restrict programs that train government authorities in Partly Free or Not Free countries on how to use social media surveillance tools.
- **Require businesses exporting dual-use technologies to report annually on the impacts of their exports.** Reports should include a list of countries to which they have exported such technologies, potential human rights concerns in each of those countries, a summary of pre-export due diligence undertaken by businesses to ensure their products are not misused, any human rights violations that have occurred as a result of the use or potential use of their technologies, and any efforts undertaken to mitigate the harm done and prevent future abuses. Further, any official government export guidance should urge businesses to exercise caution and adhere to international principles on business and human rights when exporting dual-use technologies to countries rated Partly Free or Not Free by Freedom House.

For the Private Sector

- **Limit the ability of government authorities and law enforcement to conduct blanket social media surveillance.** To the extent possible, social media companies should proactively assess and publicly disclose the different actors that can access their data through APIs (application programming interfaces) and large databases of semipublic data. Greater transparency around social media surveillance practices can help inform improved oversight and accountability mechanisms that can prevent instances where social media data is used to violate fundamental rights. Companies should also disclose and conduct due diligence on any existing and future partnerships with third parties to ensure they are not providing user information to companies that sell the data to governments of countries rated Partly Free or Not Free by Freedom House.
- **Grant users control over their information and ensure that it is not being misused**. Individuals should have the ability to see what personal data companies are collecting about them and how the data is used, as well as the ability to easily turn off data collection and tracking features. Companies also need to ensure that user data is not being used or shared in ways that customers have not explicitly authorized.

- **Train technologists and engineers on the human rights implications of the products they are building and on international best practices for preventing their abuse.** It is imperative that those building new technologies understand the ways in which the technologies can be abused or manipulated. As part of this effort, companies 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, companies should develop actionable plans to remedy any evident or potential harm.

For Civil Society

- **Work with scholars, human rights lawyers, and other stakeholders to investigate the use of social media surveillance tools and their impact on targeted communities, particularly marginalized groups.** These efforts should aim to shed light on obscure social media surveillance practices and inform advocacy and litigation on increasing transparency, oversight, and accountability.

PROTECTING INTERNET FREEDOM

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.

- **Preserve broad protections against intermediary liability and focus new regulations on conduct, not content.** Companies should continue to benefit from safe harbor protections for most user-generated and third-party content appearing on their platforms, a principle that has allowed for a historic blossoming in artistic expression, economic activity, and social campaigning. Policies designed to enforce political neutrality would negatively impact "Good Samaritan" rules that enable companies to moderate harmful content without fear of unfair legal consequences and, conversely, would open the door for government interference. In line with the Manila Principles, governments should work together with technical, legal, and human rights experts to establish meaningful oversight measures for technology companies, including the ability to evaluate companies' content moderation practices for transparency, proportionality, and the effectiveness of appeals processes.

For the Private Sector

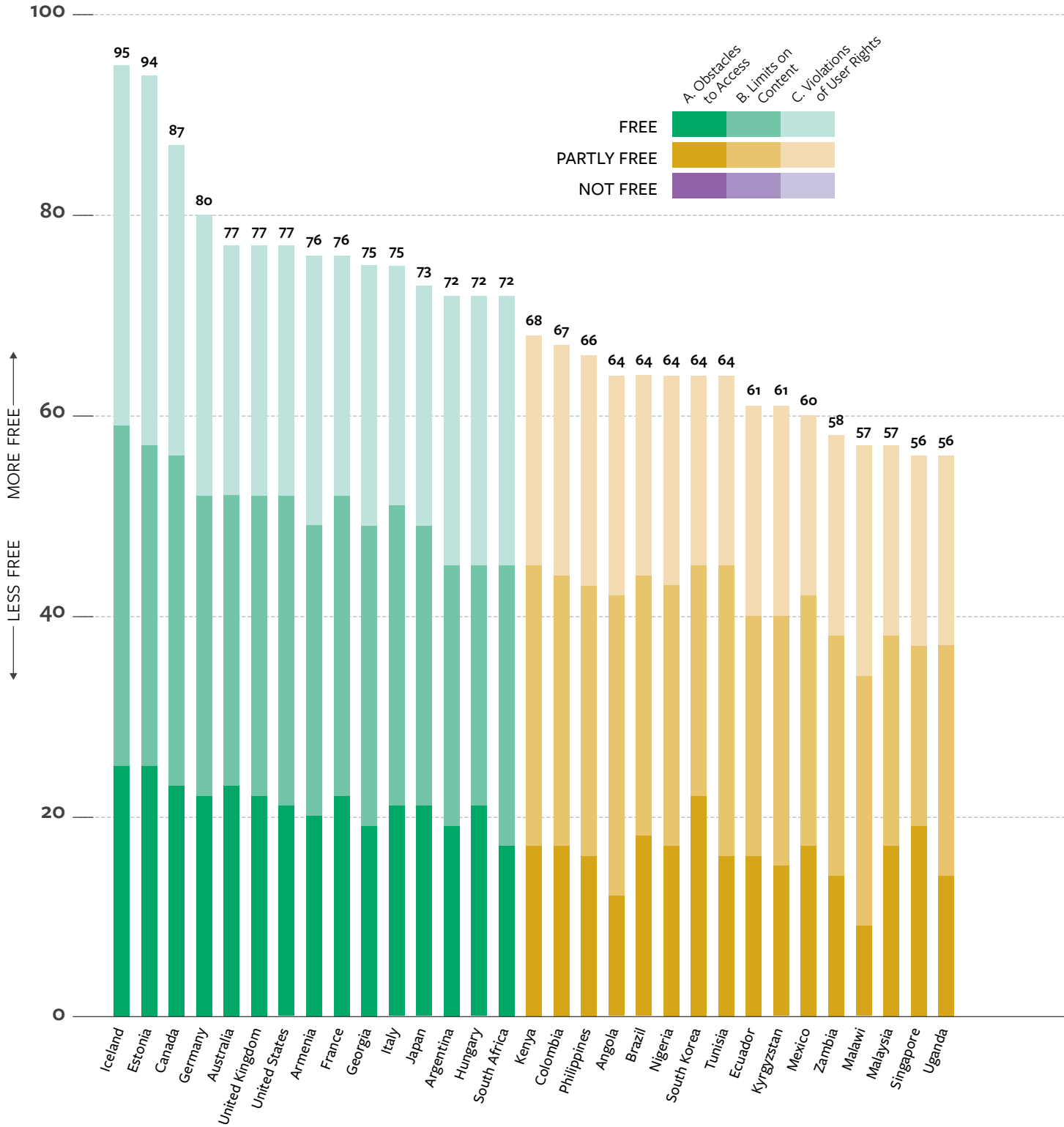
- **Adhere to the UN Guiding Principles on Business and Human Rights and conduct human rights impact assessments for new markets, committing to doing no harm.** Companies should commit to respecting the human rights of their users and addressing any adverse impact that their products might have on human rights. Companies should not build tools that prevent individuals from exercising their right to free expression, turn user data over to governments with poor human rights records, or provide surveillance or law enforcement equipment that is likely to be used to violate user rights. International companies should not seek to operate in countries where they know they will be forced to violate international human rights principles. Where companies operate, they should conduct periodic assessments to fully understand how their products and actions might affect rights like freedom of expression or privacy. When a product has been found to violate human rights, companies should suspend sales of the product to the violating actors and develop an immediate action plan to mitigate harm and prevent its further abuse.

For Civil Society

- **Continue to raise awareness about government censorship and surveillance efforts.** Civil society groups globally should engage in innovative initiatives that inform the public about government censorship and surveillance, imprisoned journalists and online activists, and best practices for protecting internet freedom, particularly in the lead-up to elections, when internet freedom violations are most acute. 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.

GLOBAL RANKINGS

0 = Least Free 100 = Most Free



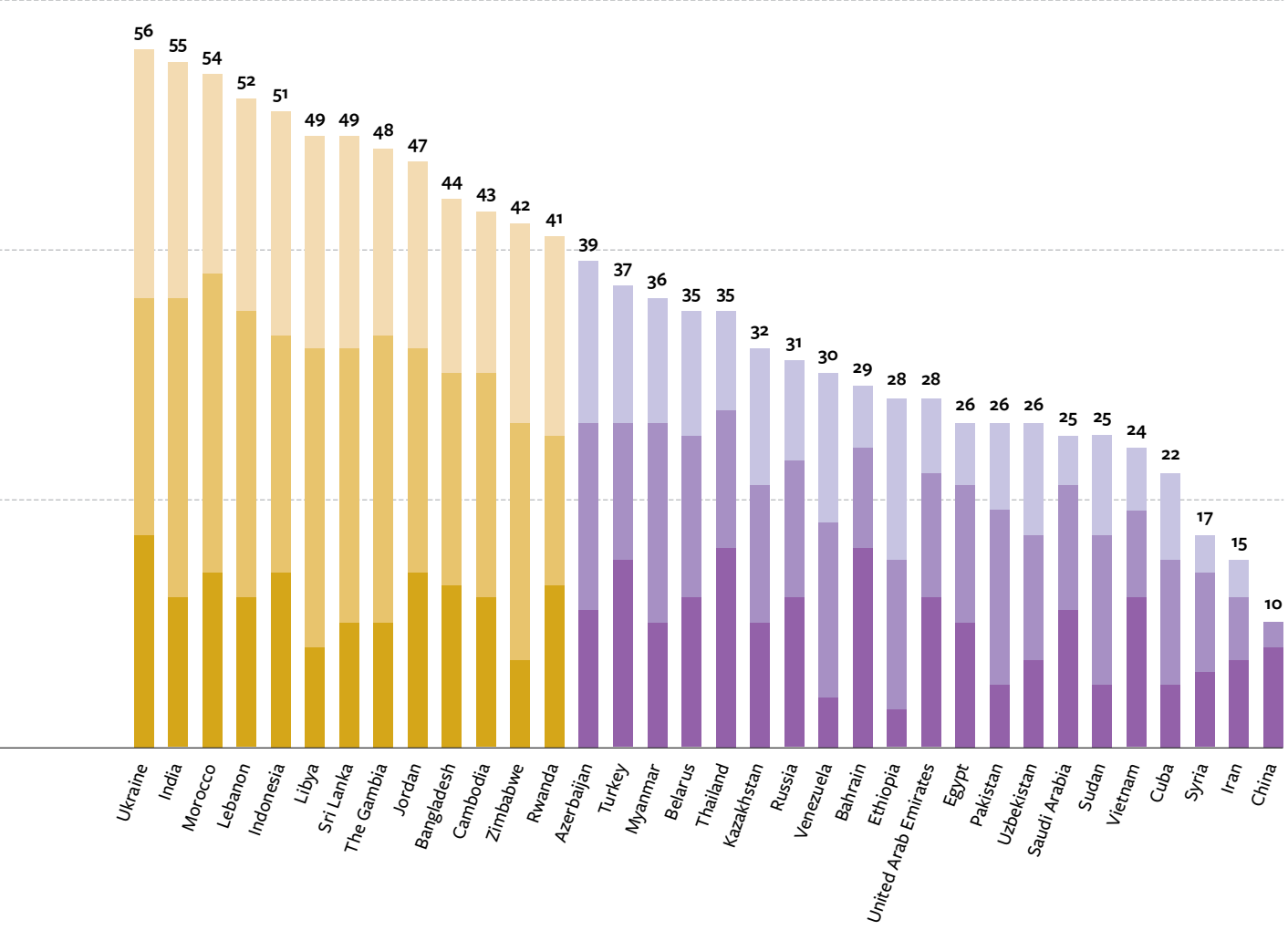
Freedom on the Net measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from **100 (the most free)** to **0 (the least free)**, which serves as the basis for an internet freedom status designation of **FREE (70–100 points)**, **PARTLY FREE (40–69 points)**, or **NOT FREE (0–39 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.



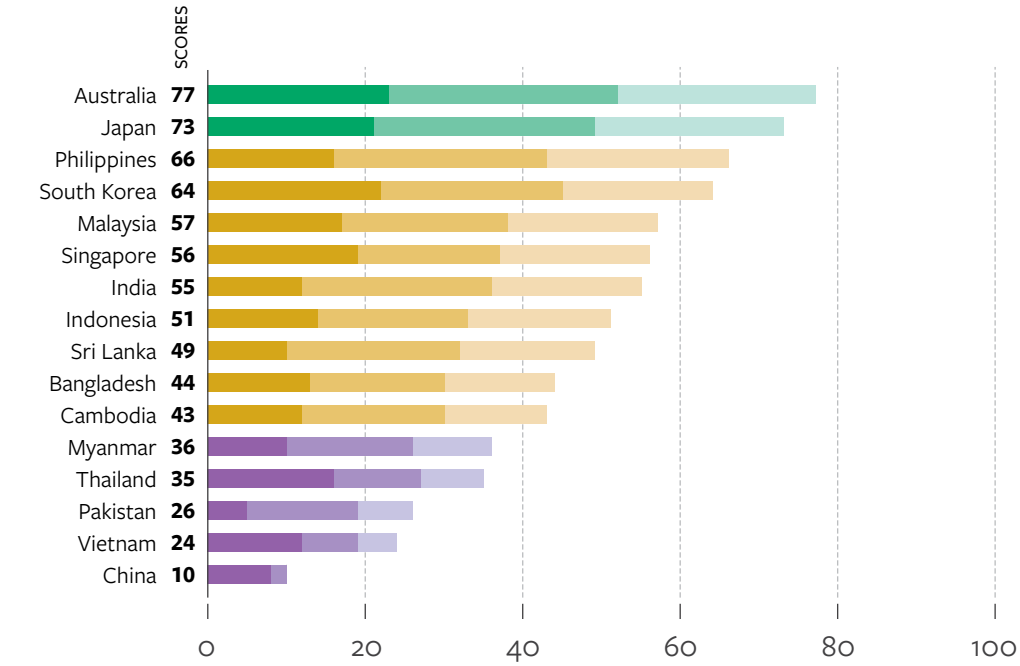
REGIONAL RANKINGS

Freedom on the Net 2019 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.

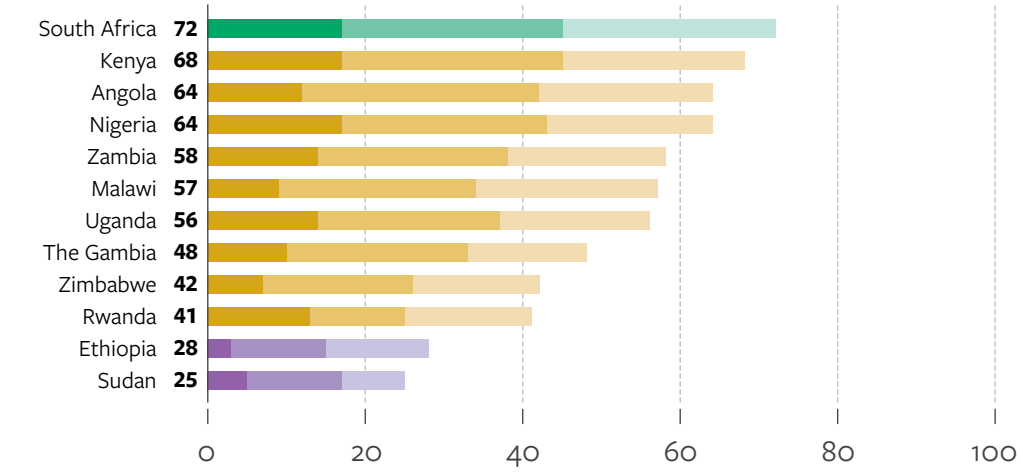
A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights

0 = Least Free
100 = Most Free

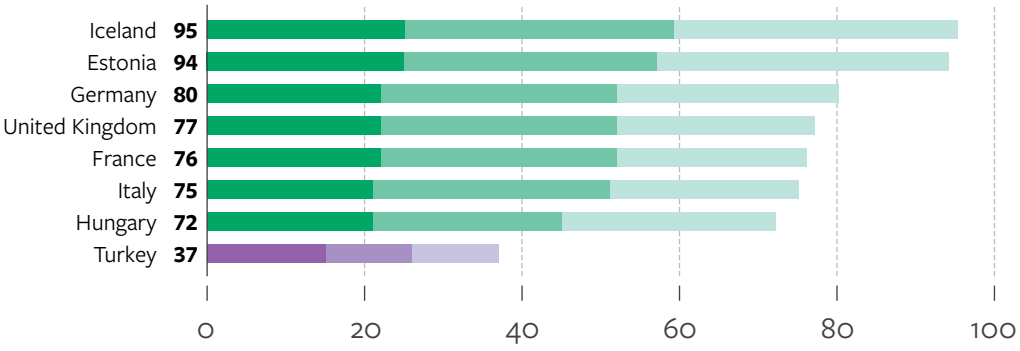
Asia-Pacific



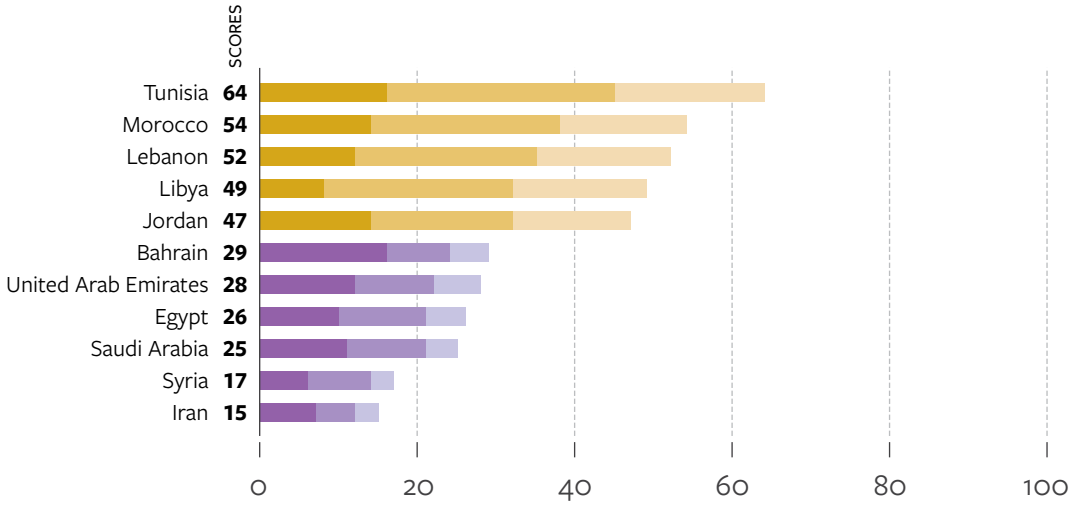
Sub-Saharan Africa



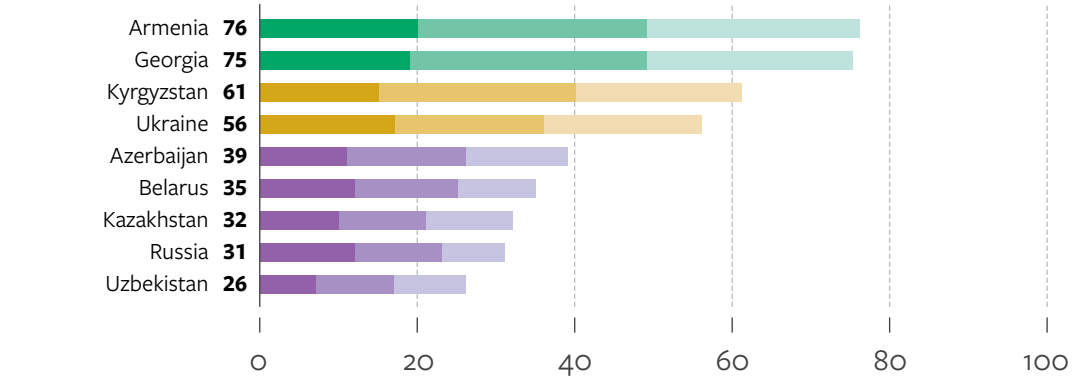
Europe



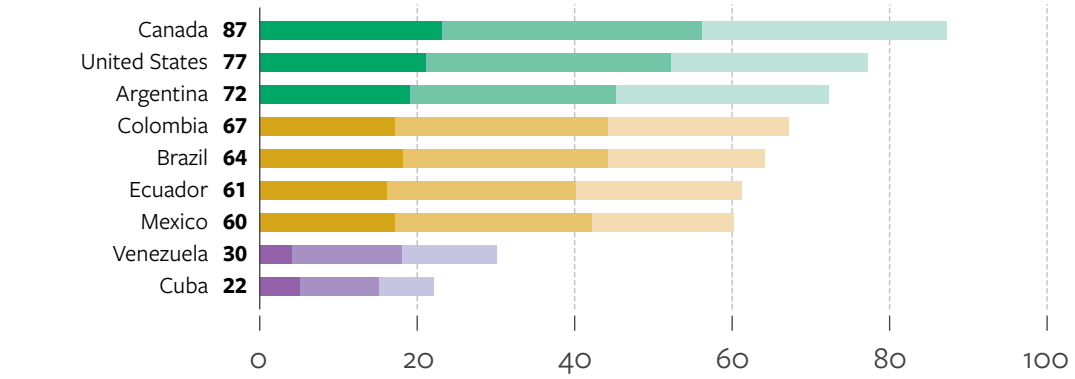
Middle East and North Africa



Eurasia



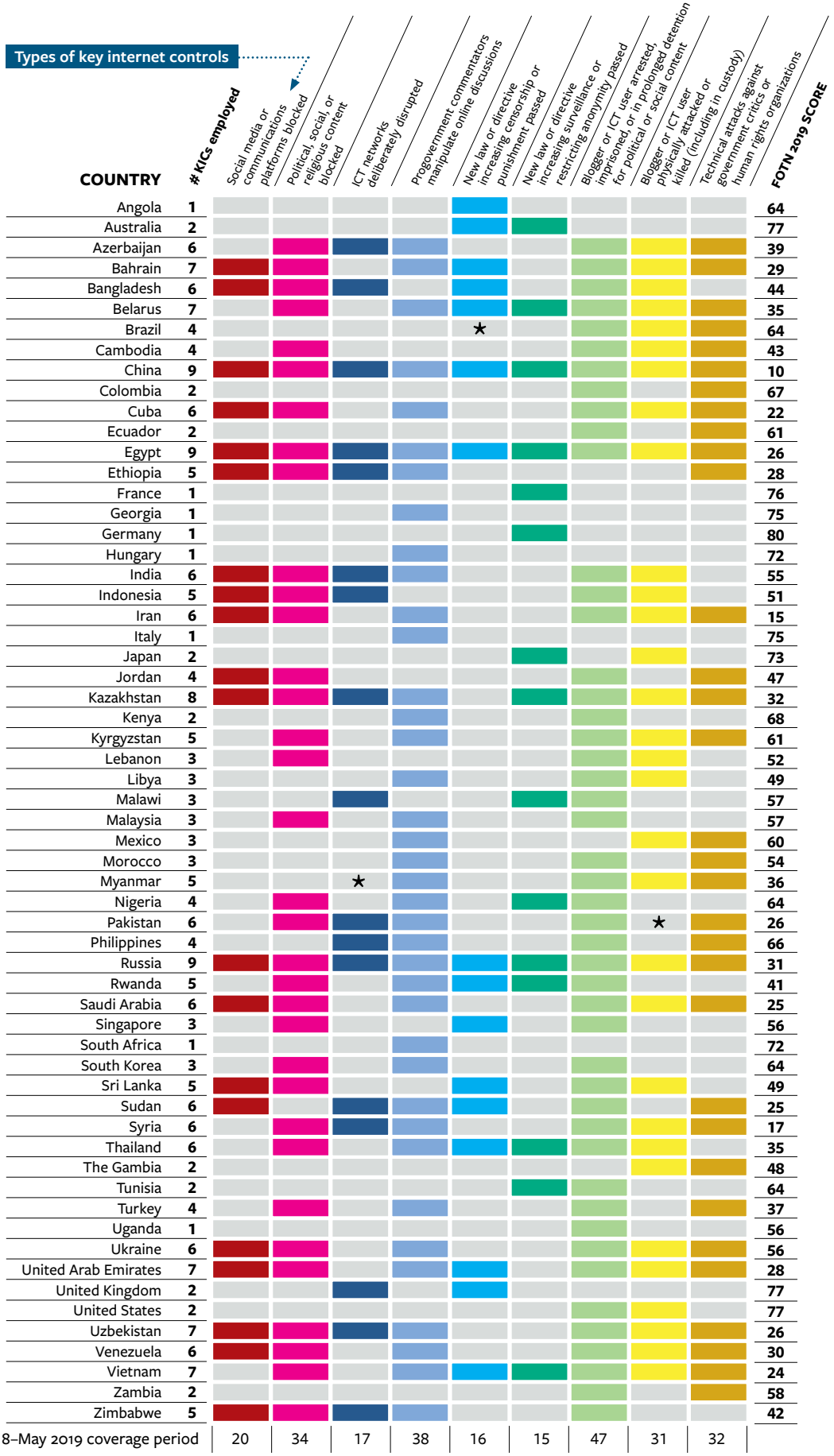
Americas



KEY INTERNET CONTROLS BY COUNTRY

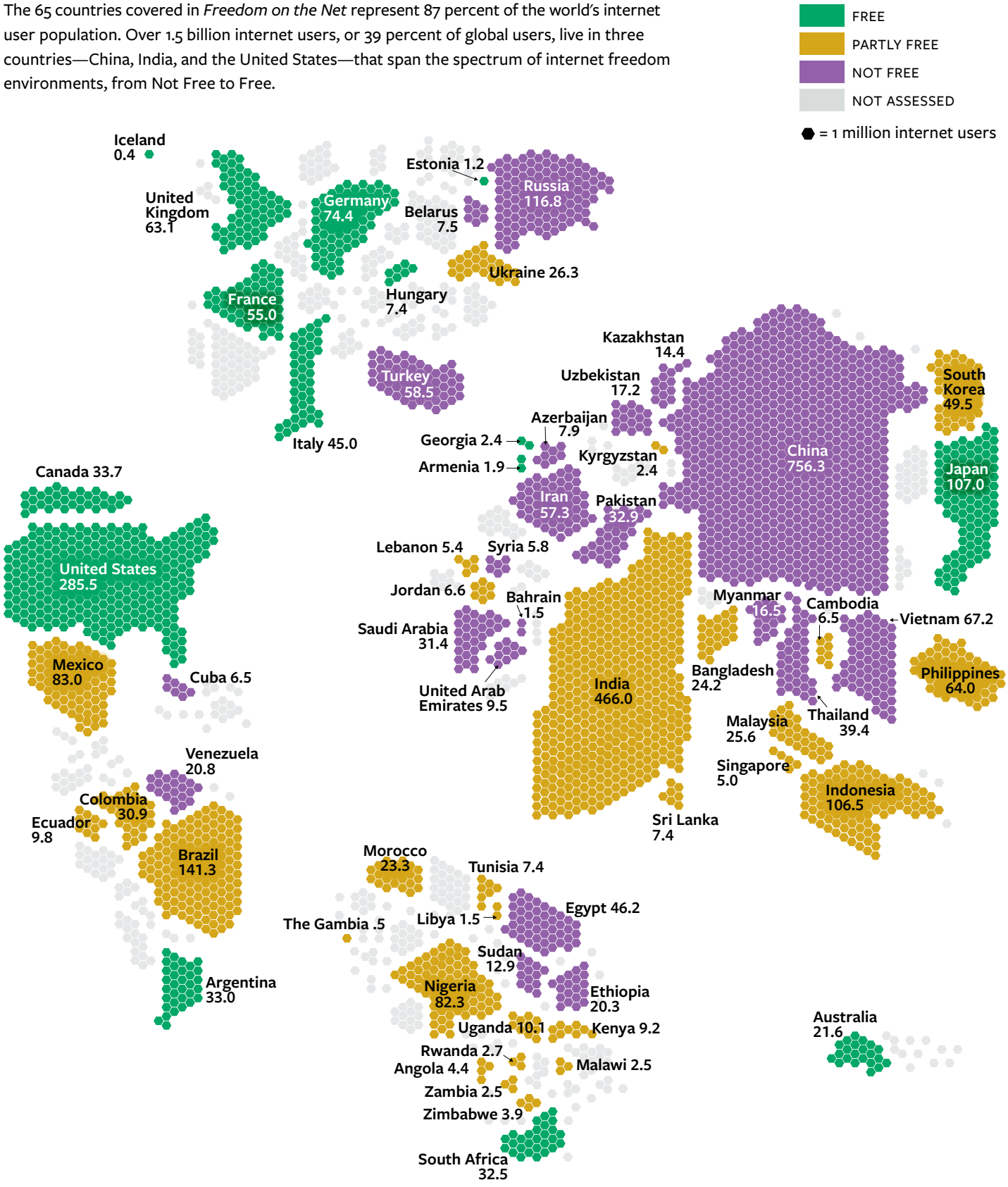
Freedom House documented how governments censor and control the digital sphere. Each colored cell represents at least one occurrence of the cited control during the report's coverage period of June 2018 to May 2019; cells with an asterisk (*) represent events that occurred between June and October 2019, when the report was sent to print. The Key Internet Controls represent restrictions on content of a political, social, or religious nature.

NO KEY INTERNET CONTROLS OBSERVED	FOTN Score
Argentina	72
Armenia	76
Canada	87
Estonia	94
Iceland	95



DISTRIBUTION OF INTERNET USERS WORLDWIDE BY FOTN STATUS

The 65 countries covered in *Freedom on the Net* represent 87 percent of the world's internet user population. Over 1.5 billion internet users, or 39 percent of global users, live in three countries—China, India, and the United States—that span the spectrum of internet freedom environments, from Not Free to Free.



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

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