

FREEDOM ON THE NET 2021

The Global Drive to Control Big Tech



FREEDOM ON THE NET 2021

TABLE OF CONTENTS

Key Findings	1
The Global Drive to Control Big Tech.....	2
The Continued Assault on Internet Freedom	4
The Promise and Peril of State Regulation	11
New laws put free expression online at risk	13
Forcing companies to hand over user data.....	16
Fostering competition to improve digital rights.....	19
Recommendations.....	25
Methodology	29
Acknowledgements	36
Tables, Charts, and Graphics	
Global Internet Population by 2021 FOTN Status.....	4
Global Internet User Stats	6
Free Expression Behind Bars.....	8
Snooping for Sale	10
Internet Regulation Sweeps the Globe	12
Best and Worst Practices for Tech Regulation.....	18
Freedom on the Net 2021 Map	22
Key Internet Controls by Country	24
Global Rankings.....	38
Regional Rankings.....	40

This report was made possible by the generous support of Amazon, the Dutch Ministry of Foreign Affairs, Google, the Internet Society, the Lilly Endowment, the New York Community Trust, the U.S. State Department's Bureau of Democracy, Human Rights, and Labor (DRL), and Verizon. Freedom House is committed to editorial independence. Our donors do not influence the organization's research priorities, report findings, or policy recommendations.

The following people were instrumental in the research and writing of this report: Grant Baker, Cathryn Grothe, Amy Slipowitz, Manisha Vepa, Kian Vesteinsson, and Tessa Weal. Elisha Aaron, David Meijer, Shannon O'Toole, and Tyler Roylance edited the report.

This booklet is a summary of findings for the 2021 edition of *Freedom on the Net*. Narrative reports on the 70 countries assessed in this study can be found on our website at freedomonthenet.org.

ON THE COVER

Illustration by Mitch Blunt

Key Findings

1

Global internet freedom declined for the 11th consecutive year. The greatest deteriorations were documented in Myanmar, Belarus, and Uganda, where state forces cracked down amid electoral and constitutional crises. Myanmar's 14-point score decline is the largest registered since the *Freedom on the Net* project began.

2

Governments clashed with technology companies on users' rights. Authorities in at least 48 countries pursued new rules for tech companies on content, data, or competition over the past year. With a few positive exceptions, the push to regulate the tech industry, which stems in some cases from genuine problems like online harassment and manipulative market practices, is being exploited to subdue free expression and gain greater access to private data.

3

Free expression online is under unprecedented strain. More governments arrested users for nonviolent political, social, or religious speech than ever before. Officials suspended internet access in at least 20 countries, and 21 states blocked access to social media platforms. Authorities in at least 45 countries are suspected of obtaining sophisticated spyware or data-extraction technology from private vendors.

4

China ranks as the worst environment for internet freedom for the seventh year in a row. Chinese authorities imposed draconian prison terms for online dissent, independent reporting, and mundane daily communications. The COVID-19 pandemic remains one of the most heavily censored topics. Officials also cracked down on the country's tech giants, citing their abuses related to competition and data protection, though the campaign further concentrated power in the hands of the authoritarian state.

5

The United States' score declined for the fifth consecutive year. False, misleading, and manipulated information continued to proliferate online, even affecting public acceptance of the 2020 presidential election results. The new administration took promising steps to enforce stronger protections for internet users.

6

State intervention must protect human rights online and preserve an open internet. The emancipatory power of the internet depends on its egalitarian nature. To counter digital authoritarianism, democracies should ensure that regulations enable users to express themselves freely, share information across borders, and hold the powerful to account.

The Global Drive to Control Big Tech

by Adrian Shahbaz and Allie Funk

In the high-stakes battle between states and technology companies, the rights of internet users have become the main casualties. A growing number of governments are asserting their authority over tech firms, often forcing the businesses to comply with online censorship and surveillance. These developments have contributed to an unprecedented assault on free expression online, causing global internet freedom to decline for an 11th consecutive year.

Global norms have shifted dramatically toward greater government intervention in the digital sphere. Of the 70 states covered by this report, a total of 48 pursued legal or administrative action against technology companies. While some moves reflected legitimate attempts to mitigate online harms, rein in misuse of data, or end manipulative market practices, many new laws imposed excessively broad censorship and data-collection requirements on the private sector. Users' online activities are now more pervasively moderated and monitored by companies through processes that lack the safeguards featured in democratic governance, such as transparency, judicial oversight, and public accountability.

The drive toward national regulation has emerged partly due to a failure to address online harms through self-regulation. The United States played a leading role in shaping early internet norms around free speech and free markets, but its laissez-faire approach to the tech industry created opportunities for authoritarian manipulation, data exploitation, and widespread malfeasance. In the absence of a shared global vision for a free and open internet, governments are adopting their own approaches to policing the digital sphere. Policymakers in many countries have cited a vague need to retake control of the internet from foreign powers, multinational corporations, and in some cases, civil society.

This shift in power from companies to states has come amid a record-breaking crackdown on freedom of expression online. In 56 countries, officials arrested or convicted people for their online speech. Governments suspended internet access in at least 20 countries, and 21 states blocked access to social media platforms, most often during times of political turmoil

such as protests and elections. As digital repression intensifies and expands to more countries, users understandably lack confidence that government initiatives to regulate the internet will lead to greater protection of their rights.

Enlisting the private sector in state abuses

The recent burst of regulatory action can be sorted into three categories pertaining to online content, personal data, and market behavior. Many of the new measures in each category could threaten the interests of users.

More governments have introduced problematic rules on removing users' speech from internet platforms. Some of the laws are designed to suppress content that is critical of the government, rather than protecting users from harmful material. Others water down due process standards by eliminating the need for a court order or mandating the use of artificial intelligence (AI) for content removal, both of which can result in significant collateral damage for political, social, and religious expression. Only in a few cases do such laws require companies to undertake meaningful transparency reporting and provide content producers with an avenue for appeal. Users are increasingly left on their own to contend with companies' murky moderation systems and protect their rights online.

A similar pattern is apparent on matters of data management. A growing number of laws facilitate government surveillance by undermining encryption and mandating that platforms store user data on servers based within the country. These localization requirements leave data especially vulnerable in settings with weak rule-of-law standards, and make it more difficult for companies to offer transnational services with strong cybersecurity features. Even laws that enshrine the rights of users to control their data often contain vague exemptions for national security, while others impose onerous licensing requirements on both local and foreign companies.

Industry regulators around the world have shown a shared zeal for cracking down on anticompetitive and abusive commercial practices. Major tech firms have received massive fines for failing to protect data and exploiting their market power to promote their own products. In a few countries, authorities worked with companies to make competing products interoperable and to allow users to switch among them more seamlessly. However, authoritarian regimes like those in China and Russia have taken heavy-handed actions with little regard for due process or the rule of law, reflecting a desire to further subordinate the private sector to the repressive political interests of the state.

Harnessing technology for democratic values

There is still time for democratic governments to pursue smart, narrowly tailored measures to protect users' rights online. Democracies should push for greater transparency and accountability regarding platforms' content moderation practices. Data privacy laws should focus on protecting users while preventing greater fragmentation of the internet. And competition policy should foster

Global norms have shifted dramatically toward greater government intervention in the digital sphere.

innovation that responds to user demand for greater personalization, security, and interoperability. Regulation should ensure that power does not accumulate in the hands of a few dominant actors, whether in government or the private sector.

The emancipatory power of the internet depends on its egalitarian nature. Wherever a user is based, a free and open internet should offer equal access to educational, creative, and communicative tools that facilitate personal and societal progress. Democratic governments have an obligation to craft regulations that enable users to express themselves freely, share information across borders, and hold the powerful to account. Otherwise, new technologies may serve to reinforce and hasten democracy's global decline.



People gather in New Delhi to protest the Indian government's use of Pegasus and other spyware to monitor citizens. Image credit: Ajay Aggarwal/Hindustan Times via Getty Images

The Continued Assault on Internet Freedom

A rundown of global findings and prominent changes to countries' internet freedom scores

Global internet freedom declined for the 11th consecutive year. The environment for human rights online deteriorated in 30 countries this year, while only 18 countries registered net gains. The largest decline occurred in Myanmar, followed by Belarus and Uganda. Ecuador experienced the largest improvement, followed by The Gambia. The United States ranked 12th overall, while Iceland was once again the top performer. For the seventh consecutive year, China was found to have the worst conditions for internet freedom.

Freedom on the Net is an annual study of human rights in the digital sphere. The project assesses internet freedom in 70 countries, accounting for 88 percent of the world's internet users. This report, the 11th in its series, covered developments between June 2020 and May 2021. More

than 80 analysts and advisers contributed to this year's edition, using a standard methodology to determine each country's internet freedom score on a 100-point scale, with 21 separate indicators pertaining to obstacles to access, limits on content, and violations of user rights. The 2021 edition includes six new countries: Costa Rica, Ghana, Iraq, Nicaragua, Serbia, and Taiwan. The *Freedom on the Net* website features in-depth reports and data on each country's conditions.

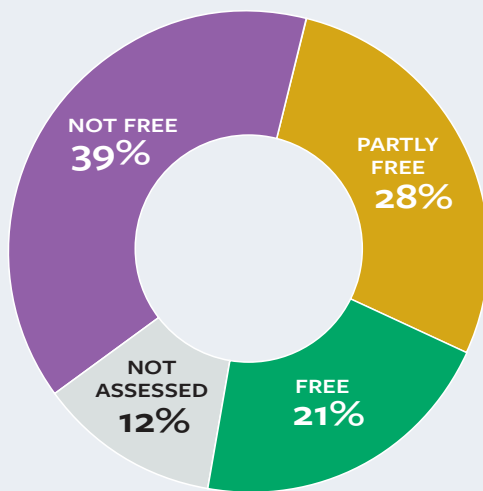
Deepening repression around electoral disputes

Internet freedom plummeted by 14 points in Myanmar—the largest decline ever recorded in *Freedom on the Net*—after the military refused to accept the results of the November 2020 general elections and launched a deadly coup in February 2021. Internet connectivity was cut off every night from then until April, and mobile services were suspended entirely beginning in March, leaving only fixed-line and wireless broadband services available to users during the day. After opposition to the coup gathered force online and overflowed into the streets, the junta also blocked social media, stripped the licenses of independent online news outlets, forced service providers to hand over personal data, and seized control of the telecommunications infrastructure. Protesters and ordinary users alike suffered physical assaults and enforced disappearances in retaliation for their online activities.

In Belarus, another electoral dispute led to a seven-point decline in internet freedom. After authoritarian incumbent Alyaksandr Lukashenka claimed victory in a fraudulent presidential election in August 2020, citizens responded with peaceful protests, and security forces embarked on a violent crackdown to quell the demonstrations. The government repeatedly restricted access to the internet,

GLOBAL INTERNET POPULATION BY 2021 FOTN STATUS

Freedom on the Net assesses 88 percent of the world's internet user population.





Protestors in Yangon shine their phone lights during a demonstration against Myanmar's military coup. Image credit: Theint Mon Soe/SOPA Images/LightRocket via Getty Images

detained and used deadly force against online activists, and ramped up social media surveillance. This repressive campaign continued into 2021, as authorities closed the offices and blocked the websites of TUT.by and Nasha Niva, two of the largest independent media outlets in the country. In May 2021, the Lukashenka regime forced a commercial plane to land in Minsk so it could arrest Raman Pratasevich, the former editor in chief of the popular NEXTA channel on the Telegram messaging platform.

Internet freedom in Uganda fell by seven points after general elections in January 2021 that were marred by irregularities. Throughout the electoral period, a network of progovernment social media accounts flooded the online environment with manipulated information, while online journalists covering the campaign of opposition candidate Robert Kyagulanyi, better known as Bobi Wine, faced harassment and physical violence. Days before polls opened, President Yoweri Museveni's government shut off the internet and blocked access to major social media platforms and circumvention tools. Facebook remained partially inaccessible for local users into the summer.

Promising breakthroughs

Ecuador registered a five-point improvement this year, in part because there was no repetition of the

intentional restrictions on internet connectivity that were imposed during mass protests against austerity measures in October 2019. The country's information space increasingly featured more diverse content, thanks largely to the efforts of citizen journalists and Indigenous netizens. Long-standing threats to internet freedom persisted, however. State actors employed dubious copyright complaints to remove critical content, and at least one journalist was briefly detained in relation to a Facebook post.

The Gambia continued an upward trend in internet freedom that began with President Adama Barrow's rise to office in 2017. The communications regulator fined a state-linked mobile service provider for unfairly manipulating voice termination rates, in a sign that the historically ineffective agency may be exercising its authority more fairly and independently. This year also featured fewer cyberattacks and instances of offline retribution for people's online activities, both of which were reported frequently during the repressive regime of former president Yahya Jammeh.

For the third year in a row, Iceland was ranked as the best environment for internet freedom, followed by Estonia. Residents of both countries enjoy high rates of access, few restrictions on content, and robust protections for

human rights online. Costa Rica, one of the first countries to recognize internet access as a fundamental right, took third place. Its legal framework includes strong guarantees for free expression and safeguards against abusive surveillance.

Taiwan enters *Freedom on the Net* with a fifth-place ranking. The country boasts a vibrant online landscape supported by meaningful and affordable internet access, an independent judiciary that protects free expression, and a lack of website blocks. Taiwanese authorities have responded to adverse Chinese government influence with innovative regulations and democratic oversight of digital technology. However, users still contend with disinformation campaigns and debilitating cyberattacks, and some individuals have faced criminal prosecutions and fines for their online speech.

A fraught environment in the United States

Internet freedom declined in the United States for the fifth consecutive year. The spread of false and conspiracist content about the November 2020 elections shook the foundations of the American political system, culminating in outgoing president Donald Trump's incitement of a violent mob to halt the certification of the election results on January 6, 2021. Several platforms took the dramatic step of deactivating Trump's accounts over the incident, which sparked renewed debate about the power of companies to police politicians' speech, as well as their responsibility to help prevent offline violence.

A raft of new proposed laws, policies, and appointments in 2021 signaled a potential shift in approach by the administration of President Joseph Biden. An executive order issued in June 2021 rescinded President Trump's August 2020 decision to halt transactions between US

The spread of false and conspiracist content about the November 2020 elections shook the foundations of the American political system on January 6, 2021.



GLOBAL INTERNET USER STATS

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

According to Freedom House estimates:

75% live in countries where individuals were arrested or imprisoned for posting content on political, social, or religious issues.

72% live in countries where individuals have been attacked or killed for their online activities since June 2020.

64% 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 access to social media platforms was temporarily or permanently restricted.

41% live in countries where authorities disconnected internet or mobile networks, often for political reasons.

individuals and entities and the Chinese-owned social media applications TikTok and WeChat—an order that a federal judge had already suspended due to First Amendment concerns. Further action against Chinese companies may be on the horizon, however, as Biden asked the Department of Commerce to investigate whether mobile apps owned by foreign adversaries presented risks to US national security and users' data privacy. In a positive move to address the country's persistent gaps in access, legislators increased funding for broadband connectivity and other internet services in a December 2020 COVID-19 relief package and in a proposed infrastructure bill in 2021.

China's ongoing digital authoritarianism

The Chinese government remained the world's worst abuser of internet freedom. New legislation criminalized expression that insults members of the armed forces, "heroes," and "martyrs." Authorities imposed draconian prison terms for online dissent, including an 18-year sentence against real-estate mogul Ren Zhiqiang, whose essay criticizing Communist Party chief Xi Jinping's handling of the COVID-19 pandemic had circulated widely online. Ordinary users also continued to face legal repercussions for mundane daily activities like sharing news stories, talking about their religious beliefs, or communicating with family members overseas. Content related to COVID-19 remained one of the most censored topics in 2021. State media outlets, official social media accounts, and other actors with suspected government affiliations flooded the information space with false claims about the danger of US vaccines and the geographical origin of the virus. The internet regulator introduced new rules to restrict independently operated social media accounts that publish about current affairs, leading to the removal of many accounts.

Nevertheless, some courageous users continued to test the boundaries of the state's internet controls. Clubhouse, a new app for real-time audio discussions, provided an unprecedented space for users to discuss sensitive issues with people outside of mainland China, until it was blocked in February 2021. A final post on the Weibo app by COVID-19 whistleblower Dr. Li Wenliang has served as a place for frustrated citizens to express themselves since his death in February 2020. And women's rights supporters pushed back against misogynistic cyberbullying and censorship by tech companies.

The Chinese government remained the world's worst abuser of internet freedom for the seventh year in a row.

Free expression in danger

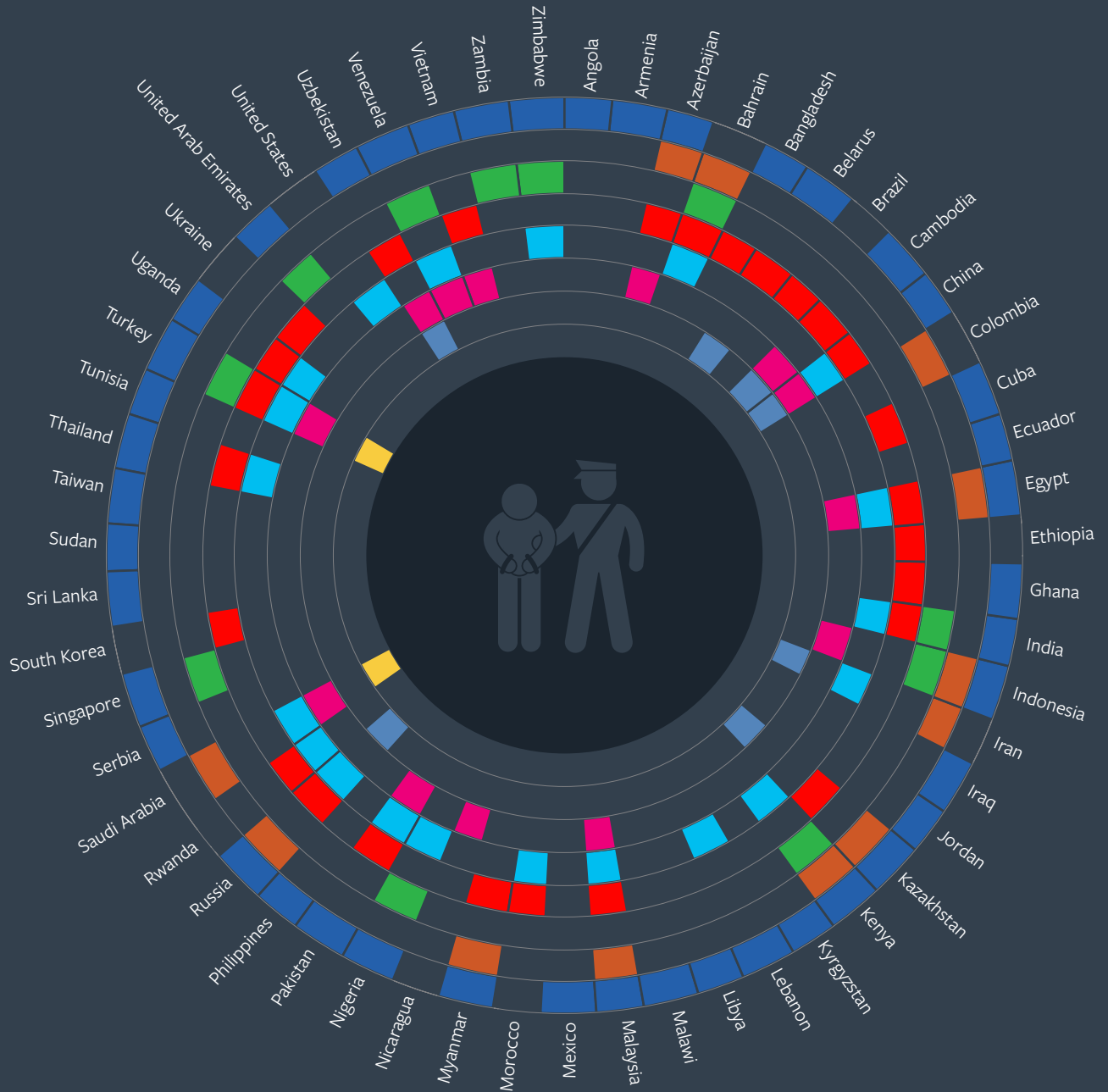
Free expression is under unprecedented strain around the world. In 56 countries, a record 80 percent of those covered by *Freedom on the Net*, people were arrested or convicted for their online speech. Several governments this year also imposed especially egregious sentences. In December 2020, Iranian authorities executed Ruhollah Zam, who administered the popular Amad News channel on Telegram, after he was accused of inciting protests and being affiliated with foreign intelligence services. In January 2021, a court in Thailand sentenced a former civil servant to 43 years in prison after she was found guilty of violating the country's draconian lèse-majesté law through her social media posts criticizing the monarchy. And in June 2021, an Egyptian court sentenced online influencers Haneen Hossam and Mawada al-Adham to 6 and 10 years in prison, respectively, for supposedly violating a human trafficking law by sharing TikTok videos that encouraged women to pursue careers on social media platforms.

This year, users faced physical attacks in retribution for their online activities in 41 countries, another record high for *Freedom on the Net*. Members of the student wing of Bangladesh's ruling party violently assaulted a Dhaka University law student in August 2020, leaving him hospitalized in critical condition, in reprisal for alleged "antigovernment activities" on social media. Local police in Azerbaijan visited a user's home in January 2021 and lured him outside by claiming to represent a municipal employment center. He was then beaten, detained, and forced to apologize for Facebook posts in which he criticized local government officials. In Mexico, Pablo Morrugares Parraguirre, founder and editor of the news site PM Noticias, was killed by unidentified gunmen in August 2020 after he stated in a Facebook video that a local gang was responsible for a taxi driver's murder.

At least 20 countries' governments shut off the internet this year, and 21 states blocked social media and communication platforms, most often during times

Free Expression Behind Bars

Government authorities investigated, arrested, or convicted people for their social media posts in at least **55 countries**.



FACEBOOK



INSTAGRAM



WHATSAPP



YOUTUBE



TWITTER



TIKTOK



TELEGRAM



CLUBHOUSE



of political turmoil such as protests and elections. In India, internet access was cut off repeatedly throughout January and February 2021 as farmers took to the streets to express their opposition to agricultural reform bills. One shutdown in Delhi affected more than 50 million mobile subscribers. The Indian government also ordered the blocking of hundreds of mobile apps owned by China-based companies amid military clashes along the Indian-Chinese border, illustrating how geopolitical tensions can erode free expression and access to information. In Ethiopia, authorities shut off the internet nationwide for at least 15 days in July 2020 following the assassination of popular ethnic Oromo singer Hachalu Hundessa and associated protests. The Ethiopian government also restricted connectivity in the Tigray Region in November 2020 as a conflict erupted between the federal government and Tigrayan forces. The shutdown continued during 2021, narrowing the flow of information in and out of the conflict area and limiting investigations into alleged atrocities perpetrated by government forces and their allies.

Spyware continues to proliferate

A booming commercial market for surveillance technology has given governments more capacity than ever before to flout the rule of law and monitor private communications at their discretion. Authorities in at least 45 of the 70 countries covered by *Freedom on the Net* are suspected of having access to sophisticated spyware or data-extraction technology supplied by secretive companies like NSO Group, Cellebrite, Circles, and FinFisher.

Limited regulation of the sale and purchase of these tools, coupled with their near ubiquity and low cost in practice, has created a crisis for human rights. Citizen Lab and Amnesty International uncovered two separate spyware campaigns targeting Indian activist Anand Teltumbde. He was subsequently arrested in April 2020, with the case reportedly relying heavily on information pulled from his electronic devices. In July 2021, Moroccan journalist Omar Radi, who had been repeatedly targeted with NSO Group's Pegasus spyware in recent years, was sentenced to six years in prison for sexual assault charges that rights groups including Freedom House have criticized as politically motivated. And an onslaught of misogynistic harassment directed at Lebanese journalist Ghada Oueiss included a personal photo that was apparently stolen from her phone using spyware.

The ongoing criminal case against French surveillance companies Amesys and Nexa Technologies shows that some form of accountability is possible for the abuses emanating from the private surveillance market. In June 2021, four executives from the companies were indicted for complicity in torture and enforced disappearances after spyware sold to Libyan and Egyptian authorities was used to identify and track down perceived political opponents.

A booming commercial market for surveillance has given governments more capacity than ever before to flout the rule of law and monitor private communications at their discretion.

The long haul of COVID-19

Throughout the coverage period, governments continued to cite the COVID-19 pandemic to justify the suppression of critical speech and the censorship of unfavorable news. In March 2021, the Cambodian government criminalized “intentionally obstructing” the implementation of COVID-19 measures, with penalties of up to five years in prison and steep fines. Subsequently, several individuals, including a member of the country's banned opposition party, were arrested for social media posts that criticized a vaccine created by a Chinese state-owned company. In July 2020, security officials in Kyrgyzstan interrogated a Facebook user for allegedly inciting hatred through his criticism of the government's COVID-19 strategy and then president Sooronbay Jeenbekov.

Smartphone apps for contact tracing, vaccine management, and quarantine compliance also continued to be deployed with few safeguards against abuse, and revelations from the coverage period clarified the ease with which public health data could be accessed for other purposes. In January 2021, the Singaporean government confirmed that data collected from the country's TraceTogether app were obtained by law enforcement bodies, spurring a public outcry that led to legal changes granting access to the data only for investigations of certain crimes. Australia's Inspector-General of Intelligence and Security reported in November

SNOOPING FOR SALE

A booming surveillance industry has allowed governments to flout the rule of law and monitor private communications at their discretion.



2020 that intelligence agencies had incidentally collected data from the country's COVIDSafe app.

In a welcome development, a small number of governments rolled back problematic pandemic-related states of emergency that had unduly restricted free expression, while others ended overly broad data-sharing programs. In June 2020, an Argentine municipal government repealed an ordinance that fined users for sharing false information

about COVID-19 after the law was enforced against journalists. Upon renewing its COVID-19 emergency powers in September 2020, the government of the Philippines omitted previous provisions that had criminalized online speech. And Armenia's government ceased its collection of metadata, including location and phone-record data, from telecommunications companies for ostensible contact-tracing purposes; the hardware devices that stored the information were then physically destroyed.

The Promise and Peril of State Regulation

Global norms have shifted toward greater state intervention in the digital market. At least 48 countries pursued legislative or administrative action aimed at regulating technology companies over the past year. This trend comes amid calls to address societal problems that are exacerbated online, such as harassment, extremism, and serious criminality, and to better protect users from fraudsters, foreign adversaries, and exploitative business practices. While a few measures introduced this year have the potential to hold tech giants more accountable for their performance, most simply impose state and even political responsibilities on private firms without securing greater rights for users.

The impact of new laws and regulations on human rights varies from country to country. In robust democracies, well-crafted requirements for platforms have the potential to mitigate online harms while bolstering transparency and accountability. Analogous laws, however, may be abused by illiberal politicians and authoritarians to remove nonviolent political, social, and religious expression. Most alarming are those that bring the private sector further under the authority of the state in a bid to more effectively stamp out dissent, conduct blanket surveillance, and disseminate propaganda. In China, for example, local tech firms are punished not only for lax data security and monopolistic practices, but also for failing to remove cartoons that



A demonstrator in Lagos holds a sign advocating for digital rights amidst nationwide protests over the Nigerian government's Twitter ban. Image credit: PIUS UTOMI EKPEI/AFP via Getty Images

INTERNET REGULATION SWEEPS THE GLOBE

Governments in at least 48 countries pursued new rules for tech companies on content, data, and competition over the past year.



mock Xi Jinping and testimony from Uyghurs about arbitrary detentions in Xinjiang.

It is undeniable that the unregulated growth of the tech industry has given a small number of firms an astounding ability to monitor and influence the behavior of billions of people. On January 6, 2021, this power was in full view as Facebook, Twitter, and several other platforms took the dramatic decision to deactivate the accounts of outgoing US president Donald Trump. The president's rhetoric had plainly contributed to the violent insurrection at the US Capitol, leading many to welcome the bans and suspensions in Trump's case. The tech companies, however, were not clear or consistent about how they

treated speech by influential politicians. In fact, they had long been dogged by accusations of arbitrary takedowns in other contexts, affecting journalists, human rights defenders, and members of marginalized communities around the world. Such incidents have strengthened the argument that major platforms cannot be relied upon to moderate content without some sort of oversight.

Yet as companies respond to public criticism by stepping up enforcement of their own community standards against false and violent rhetoric, they face increasingly tense showdowns with illiberal and authoritarian governments. Where democratic checks and balances are lacking, government officials will exploit regulation to punish any

company that moderates politicians' speech, or pushes back against arbitrary orders to remove content or hand over data. This year, officials in India pressured Twitter to remove protest-related and critical commentary and to stop flagging manipulated content shared by the ruling party. Nigerian authorities blocked Twitter after the company removed incendiary posts by the country's president. Turkish president Recep Tayyip Erdoğan, who himself has overseen the mass incarceration of journalists and opposition politicians, repeatedly accused tech companies of "digital fascism" for their refusal to comply with flawed provisions in the country's new social media law. As an alternative to US firms, Erdoğan has promoted a state-owned messaging platform, while both Indian and Nigerian officials have migrated to Koo, a Bangalore-based app.

A vibrant democracy requires laws and institutions that guard against the accumulation of power in the hands of a few, whether in government or the private sector. The current drive for greater regulation raises the risk that instead of curbing and decentralizing the power of tech companies, governments will attempt to wield it for their own purposes and further infringe on users' rights. The most promising legislation seeks to address online ills while bringing both corporate and state practices into compliance with international human rights principles such as necessity, transparency, oversight, and due process. But the danger posed by the worst initiatives is immense: if placed in the hands of the state, the ability to censor, surveil, and manipulate people en masse can facilitate large-scale political corruption, subversion of the democratic process, and repression of political opponents and marginalized populations.

New laws put free expression online at risk

Authorities in at least 24 countries passed or announced new laws or rules governing how platforms treat content. They variously include requirements to take down illegal content, penalties for certain forms of removals, the appointment of legal representatives to manage state requests, and stronger transparency and due process provisions. The most problematic measures may result in increased censorship of political dissent, investigative reporting, and expressions of ethnic, religious, sexual, or gender identity, particularly among marginalized communities.

The drive for greater regulation raises the risk that instead of decentralizing the power of tech companies, governments will attempt to wield it.

Problematic obligations to remove content

India's new social media regulations represent one of the most comprehensive initiatives during this report's coverage period. The updated Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules include new obligations for social media intermediaries, an expanded grievance mechanism through which users can complain directly to companies, and a reduced window for responding to law enforcement requests. Significant social media intermediaries—defined as companies with at least five million users—are required to deploy AI-based moderation tools, open in-country offices, and appoint three new local officers. A chief compliance officer, for example, must comply with takedown orders from a court, government agency, or any other competent authority within 36 hours, and can be held personally liable and face prison terms of up to seven years for failure to do so.

The Indian rules provide some improvements to platforms' content moderation by requiring that significant social media intermediaries notify users when their content is removed, communicate a clear justification for the decision, and provide an avenue for appeal. However, the expanded obligations imposed on social media platforms, coupled with the in-country representative requirements and the risk of criminal liability, will curb companies' willingness to push back against state censorship requests that do not meet international human rights standards. Indian law bans a broad array of vaguely defined content, including speech that undermines public order, decency, morality, or the country's sovereignty, integrity, and security. The user reporting mechanisms could also be abused by the government's partisan supporters to remove critical commentary.

The rules were announced amid worsening relations between the ruling Bharatiya Janata Party and Silicon Valley. During large protests against proposed agricultural reforms in February 2021, Twitter reversed its initial decision to fully

India's Intermediary Rules were announced amid worsening relations between the ruling Bharatiya Janata Party and Silicon Valley.

comply with a government order to remove the accounts of journalists and activists. Over the following months, Twitter faced police inquiries and a visit to its offices, threats that its employees would be criminally charged, and claims by authorities that the platform had lost immunity from liability for user-generated content. Throughout the spring, the government ordered Facebook, Twitter, and Instagram to remove content criticizing authorities' handling of a deadly surge in COVID-19 infections.

Turkey's new social media regulations came into effect in October 2020. Platforms with over a million daily users are required to remove content deemed "offensive" within 48 hours of being notified, or risk escalating penalties including fines, advertising bans, and limitations on bandwidth. The platforms are also required to appoint a Turkish national as an in-country representative or establish a local legal entity, which is then subject to judicial fines for failure to comply with legal orders to remove content. The law reduced social media companies' ability to resist requests from Turkish authorities that are designed to further censor opposition voices, independent journalism, and nonviolent expression. Most companies have since established a legal entity, though some have promised that there will be no change to their content moderation policies.

Similarly, Indonesia's Ministerial Regulation 5, enacted in November 2020, places new takedown and registration requirements on a broad array of tech companies regardless of their size, including social media apps, content-sharing services, and search engines. Once notified, a platform has only four hours in "urgent" situations or 24 hours otherwise to remove "prohibited" content, broadly conceptualized as speech that violates any domestic law, creates community anxiety, or disturbs public order. Authorities have already applied existing laws to censor LGBT+ content, criticism of Islam, and commentary about an independence movement in the provinces of Papua and West Papua. Those not in compliance with the new regulation risk a range of penalties that include blocking and revocation of licenses. In addition

to human rights concerns regarding its expansive scope, the regulation's tight removal deadlines raise the question of whether any but the largest companies have the resources to comply and thus survive in the Indonesian market. The deadlines also incentivize companies to deploy automated monitoring systems that often excessively or inconsistently flag and censor users' speech.

The Russian government added to the labyrinth of regulations that international tech companies must navigate in the country. A January 2021 law introduced new fines for websites and platforms that fail to remove content the state deems "illegal," while a February law reinforced platforms' obligations to identify and remove banned content and required them to coordinate with the federal regulator, Roskomnadzor, regarding content moderation decisions. The simmering tension between foreign platforms and the Russian state came to a boil in March, when Roskomnadzor throttled Twitter's traffic over the company's failure to comply in full with orders to remove information related to protests against the detention of opposition leader Aleksey Navalny.

Australia and the United Kingdom introduced legislation intended to address concerns about online safety. Australia's Online Safety Act, adopted in June 2021, empowers an eSafety Commissioner to order companies to remove content—vaguely described as image-based abuse, cyber abuse, cyberbullying, or otherwise harmful material—within 24 hours. By requiring such rapid takedowns and including unclear definitions of prohibited content, the law risks disproportionately affecting the legitimate speech of marginalized groups, including sex workers and educators, LGBT+ communities, and artists. The law also lacks accountability for how the commissioner makes decisions, provides little opportunity for users to respond to complaints about their content, and encapsulates a variety of different internet companies instead of differentiating obligations based on their size and function. The United Kingdom's Online Safety Bill, which had yet to pass at the time of writing, also places the duty of care on content providers to ensure that their users are not exposed to either illegal or harmful content, which are not clearly defined.

Misguided anticensorship laws

The decision by several major platforms to deactivate the accounts of outgoing president Trump in January 2021 sparked numerous bad-faith attempts at regulation, particularly in countries where populist leaders have relied on the power of social media to dominate public discourse.

Weeks after Trump was banned, the Russian parliament announced plans for a law that would impose fines on companies for blocking users illegally. President Vladimir Putin had already signed a law in December that allows authorities to block platforms for restricting content from Russian state news outlets. That law cited instances in which Twitter, Facebook, and YouTube had “censored” the state-affiliated outlets RT, RIA Novosti, and Crimea 24. Facebook and Twitter had previously introduced labels for state-affiliated media groups, identifying RT and RIA Novosti as being closely associated with or under the direct editorial control of the Russian government.

Mexican president Andrés Manuel López Obrador similarly lambasted social media companies as “global institutions of censorship” after the ban on Trump, suggesting the creation of a new state-owned service as an alternative. A few weeks later, Mexico’s Senate Majority Leader proposed draft legislation that grants the country’s regulator broad authority to overturn social media companies’ content moderation decisions without judicial oversight, including the power to order the restoration of users’ accounts or content if they were removed. In addition to prohibiting the removal of content not outlined in the bill, the legislation would require platforms to restrict content that the regulator deems to be hateful, false, or threatening to public

order. Companies that fail to comply would face fines of up to \$4.4 million.

In September 2021, Brazilian president Jair Bolsonaro signed new rules that modify the country’s Marco Civil da Internet, one of the world’s most comprehensive laws protecting human rights online. Social media companies can now restrict users’ accounts and content only under very narrow circumstances, for instance if the material involves nudity or violence, or when acting on a court order. The president’s decree effectively limits companies’ ability to enforce their own terms of service by curbing health misinformation or falsehoods that sow doubt about the electoral process—both of which Bolsonaro himself has actively disseminated.

A more promising focus on transparency and due process

The European Union (EU) framework for internet regulation may offer a “third way” between China’s digital authoritarianism and the traditional US emphasis on unrestricted speech and free markets. Two pieces of EU legislation introduced this year—the Digital Services Act (DSA) and the Digital Markets Act—promise to set some positive rules for the tech sector, although democratic policymakers should remain wary of the negative



The executive vice president and competition commissioner of the European Commission, Margrethe Vestager, and the internal market commissioner, Thierry Breton, unveil the EU’s new Digital Services Act and Digital Markets Act in Brussels, Belgium. Image credit: Alexandros Michailidis/Straight Out Of The Camera/Bloomberg via Getty Images

repercussions that their laws could have on internet freedom in more closed environments. Germany's 2018 Network Enforcement Act (NetzDG), for example, introduced problematic requirements for companies to expediently remove content without a court order and establish a local legal presence. While the law has since been amended, the original has been mimicked and misused by backsliding democracies and authoritarian regimes in order to force social media providers to remove LGBT+ content and investigative journalism. Similarly, authorities in several countries cited the EU's 2018 General Data Protection Regulation (GDPR) to stymie cross-border data flows and support vague exemptions for state surveillance.

The DSA requires large intermediaries to produce detailed reports on a broad range of their practices, including content moderation, algorithmic curation and recommendation systems, and online advertising. Due process protections would also be bolstered under the law. Users would be notified about moderation decisions affecting their content and provided with an appeals process. However, the proposal builds on the controversial "notice-and-action" framework first introduced in the US Digital Millennium Copyright Act (DMCA) of 1998, which created a standard mechanism for copyright owners to request the removal of infringing materials from platforms without a court order. The DMCA suffers from challenges in issuing counternotices and documented abuse by politicians seeking to remove unfavorable content. Attention is needed to ensure that the DSA addresses these shortcomings and does not become a global model for censoring political expression.

In the United States, revisions to the draft Platform Accountability and Consumer Transparency Act pushed the legislation in a positive direction following feedback from civil society. The bipartisan measure requires companies to publish details about their moderation practices, institute due process protections for users, and remove content deemed illegal by a court within four days. This bill largely avoids the missteps of many more problematic proposals to reform Section 230 of the Communications Decency Act, which has long shielded providers and content hosts from legal liability for most material created by users.

Taiwan's draft Internet Audiovisual Service Management Act would enhance transparency about streaming platforms' operations in the country by mandating that certain companies report revenue and user statistics, provide an easy-to-use user complaint mechanism, and ensure that their

terms of service clarify how data are collected and used, among other policies. The bill was introduced amid concerns that streaming platforms owned by China-based companies were operating illegally in Taiwan and could facilitate the spread of disinformation or other manipulated content emanating from Beijing.

Forcing companies to hand over user data

In at least 38 of the 70 countries assessed this year, governments initiated legal or administrative reforms affecting tech companies' management of user data. Major platforms have often been prohibited by their home country's laws from handing over data to foreign officials. The governments seeking information are now attempting to sidestep these jurisdictional barriers by forcing companies to store data on servers based within their borders, surrender personal data to law enforcement agencies with limited oversight, and circumvent the encryption of private communications. Particularly in countries with poor human rights records, domestic data storage significantly expands the potential for surveillance and the risk of abuse. These problematic provisions are sometimes paired with more positive requirements for companies to protect users' data from other threats.

Data sovereignty as an excuse for surveillance

A draft decree released in February 2021, as part of the implementation of Vietnam's Cybersecurity Law, expands requirements for large and small online platforms to store data on Vietnamese servers, including users' names, birth dates, nationality, identity cards, credit card numbers, biometric files, and health records. Authorities can access user data under vaguely defined pretexts related to national security and public order. Full compliance with Vietnamese law by social media companies would put activists, journalists, and human rights defenders at risk, given the one-party regime's harsh suppression of perceived political dissent.

Interim regulations published in Saudi Arabia in October 2020 aim "to ensure preservation of the digital national sovereignty over data." Companies and government entities must obtain written approval from the government regulator before processing or transferring personal data outside of the country. Meanwhile, new data protection regulations enacted in Dubai, in the United Arab Emirates, require the

local storage of any “secretive, sensitive, and confidential” data pertaining to individuals and companies. A new data protection bill proposed in October 2020 in Bangladesh would also require domestic data storage.

In some cases, such data localization requirements have been introduced in the context of content regulation. Pakistan’s proposed Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, the latest version of which was published in November 2020, outlines requirements for social media companies to establish one or more data servers in the country. Similarly, Turkey’s social media law requires platforms to store data locally and establish domestic legal representatives or face five stages of escalating penalties, including fines, an advertising ban, and bandwidth limitations of up to 90 percent.

Data protection policies may also be used to place stringent limitations on cross-border data transfers and impose onerous licensing requirements on companies. Under a data protection law ratified in Egypt in July 2020, domestic and foreign entities must obtain a state license and appoint a local data protection officer to conduct cross-border data transfers. Unlike the independent commissions formed in many democracies, Egypt’s data protection agency will be supervised by a board comprising representatives of government ministries, including security and intelligence officials. The law’s exorbitant licensing fees are prohibitive for many small and medium-sized enterprises.

Continuing pressure on encryption

In addition to requiring data localization, many new regulations threaten to undermine encryption, which is essential for data privacy and cybersecurity and a critical tool for journalists and human rights defenders around the world. India’s revised Information Technology Rules require large social media platforms to identify and disclose the “first originator” of a message if requested by the government or judiciary in cases related to state sovereignty, security, public order, and sexually explicit content. Companies would effectively have to dismantle end-to-end encryption in order to unmask a message’s originator, undermining the privacy and security protections on which users, companies, and governments have come to rely. In May 2021, WhatsApp sued the government to halt the rules’ implementation, arguing that the traceability requirements violated constitutionally guaranteed privacy protections.

The proposed Brazilian Internet Freedom, Responsibility, and Transparency Act includes similar yet more narrow traceability requirements. Private messaging services would be required to store for three months the traceability data of messages that go viral, defined as those forwarded by more than five users and that reach at least 1,000 accounts. While this provision is significantly scaled back from one in an earlier draft, companies would still in practice have to erode encryption to trace and identify messages that reach the low virality threshold.

Democratic leaders disparaging end-to-end encryption serves the interests of more authoritarian governments that seek to undermine the technology for their own political ends.

Pakistan’s proposed rules have raised alarms about their impact on end-to-end encryption. The draft requires social media companies and service providers with more than 500,000 users to hand over personal data in a decrypted and readable format when requested by the Federal Investigation Agency. Similarly, amendments to the Nigerian Broadcasting Code proposed in August 2020 require broadcasters to comply with decryption orders during moments of emergency.

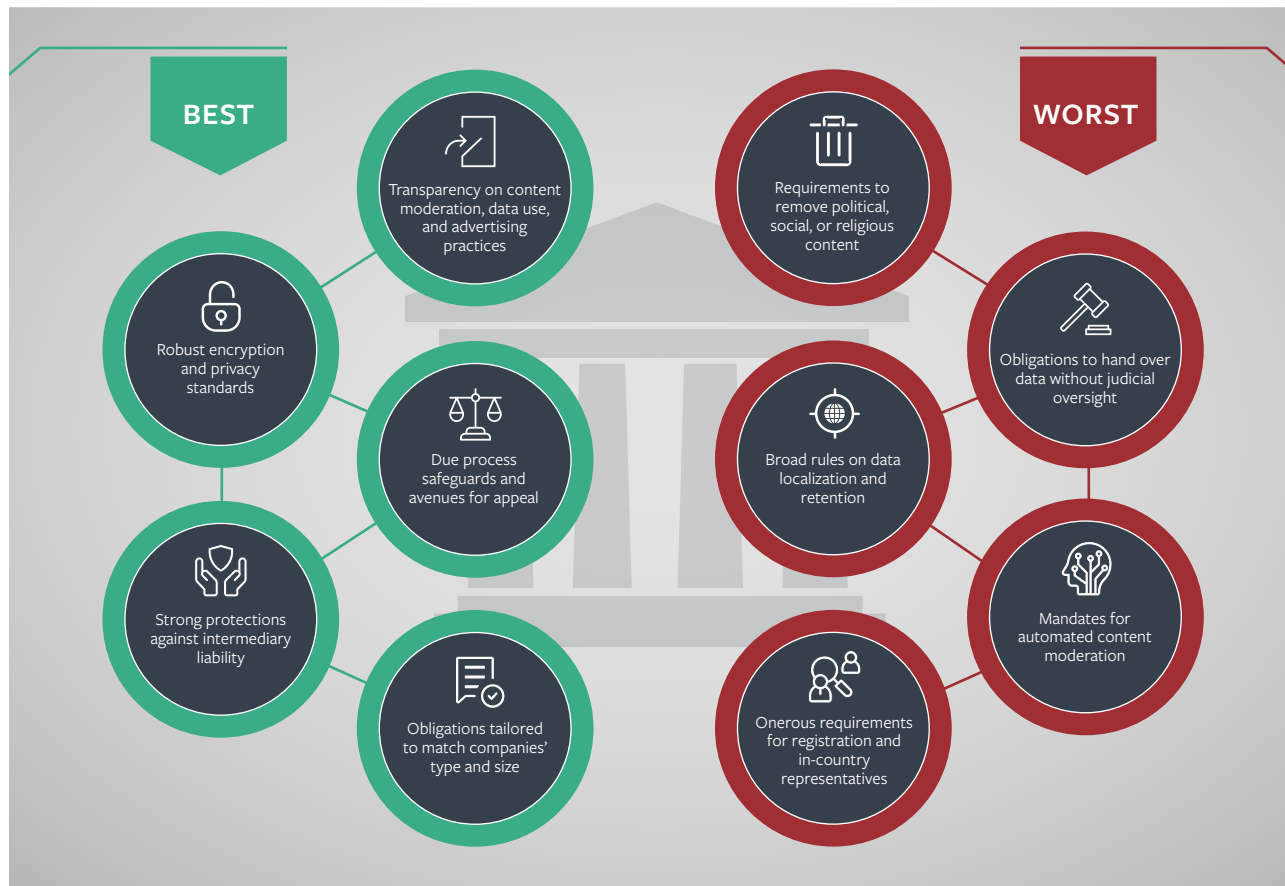
Over the past year, democratic leaders again disparaged end-to-end encryption, serving the interests of more authoritarian governments that seek to undermine the technology for their own political ends. For example, in October 2020 leaders from Japan, India, and the Five Eyes—an intelligence alliance composed of the United States, the United Kingdom, Canada, Australia, and New Zealand—decried encryption as an impediment to national security, criminal, and child sexual abuse investigations. But any weakening of encryption protocols or requirements for “backdoor” access would effectively undermine the security of civil society groups, businesses, and ordinary users, potentially endangering lives.

Contrasting dynamics in China

In China, growing public anger at a series of data scandals has put authorities under greater pressure to limit companies’ exploitation of user information. This year’s Personal

BEST AND WORST PRACTICES FOR TECH REGULATION

Some new laws are designed to bolster human rights. Others feature provisions that can be exploited to subdue free expression and increase surveillance.



Information Protection Law, which draws on the EU's GDPR framework, is the country's first comprehensive attempt at limiting how companies collect, store, and use personal data. A regulation introduced in March 2021 limited the types of data that apps can require from users. Regulators subsequently alleged that over 100 apps—including those from Chinese tech giants Tencent and Baidu—violated the rules. In July, authorities asserted that the ride-hailing app Didi illegally collected users' personal information. Didi was pulled from China-based app stores, and a scheduled initial public offering on a US stock exchange was canceled. Authorities also passed a Data Security Law this year that requires Chinese companies to obtain approval from the state prior to sharing data with a foreign judicial or law enforcement entity.

At the same time, China is home to the world's largest surveillance state. Under its Cybersecurity Law, implemented

in 2017, companies must store users' data on local servers and decrypt the data on request from the authorities. Vague laws enable state agencies to monitor the population for an expansive list of activities and ideas that are deemed harmful by the one-party regime. In practice, this includes political, social, and religious expression, independent reporting, and the online activities of marginalized groups, for which users can face draconian criminal penalties.

Protecting users' data

Some new data protection laws introduced during the coverage period established meaningful constraints and oversight on how private companies access, store, and use personal information, without further empowering the state to monitor its citizens. In Ecuador, nearly two years after a sprawling data breach revealed over 20 million people's

information, the government adopted a new data protection law in May 2021. The law, one of the most robust of its kind in Latin America, creates a new data protection agency, regulates cross-border transfers, and requires companies to provide users with the ability to access, amend, or delete their information. Although it strongly resembles the GDPR, the Ecuadorean law prescribes significantly lower fines for noncompliance compared with the EU regulation.

Several governments over the past year also investigated or fined companies for their misuse of data. In December 2020, France's data protection agency fined Google €100 million (\$120 million) and Amazon €35 million (\$41.9 million) for breaching the country's French Data Protection Act. Italy's data protection authority fined the telecom provider Wind €17 million (\$20.3 million) for unlawful data processing and the provider Iliad €800,000 (\$958,000) for violating the GDPR in July 2020.

Fostering competition to improve digital rights

In at least 21 countries over the past year, authorities proposed action against companies to defend competition in the digital market. Governments around the world recognized that market forces, when left unchecked, pose a threat to users' rights. Regulators are employing competition policy as a tool to prevent abuse of user data, strengthen the information space, and empower users with greater choice.

Governments around the world recognized that market forces, when left unchecked, pose a threat to users' rights.

Like anticorruption campaigns, however, competition policy may also be wielded in a politically motivated manner. As more governments build their capacity to regulate digital markets, it is vital that they adhere to good governance and human rights principles regarding necessity, proportionality, and transparency in order to ensure that both state and corporate power remain accountable to the public.

Democracies ramp up scrutiny of business practices

The proposed Digital Markets Act, unveiled by the EU in December 2020, is a sweeping effort to set clear, consistent, and rights-respecting rules. The draft legislation reclassifies certain service providers as “gatekeepers.” Such companies are prohibited from ranking their own products ahead of competitors and preinstalling their own apps on devices. The bill also provides users with the ability to transfer their data across services, a feature known as data portability.



A New York train passenger reads a newspaper reporting on big tech company executives testifying to a congressional committee investigating monopoly policies. Image credit: Robert Nickelsberg via Getty Images

Germany passed similar provisions in a January 2021 Digitalization Act that grants the Federal Cartel Office (FCO) greater authority to investigate companies' behavior, with a specific mandate to ascertain whether they are denying interoperability, preinstalling apps, preventing competitors from advertising, or failing to provide users with agency to determine and understand how their data are processed. After the passage of the law, the FCO launched investigations into market behavior by Amazon, Apple, Facebook, and Google. The UK Competition and Markets Authority announced in June that it would play an active role in shaping Google's new Privacy Sandbox feature to ensure that replacements for cookie tracking, meant to protect privacy, do not harm competition.

Antimonopoly action also intensified in the United States. Under new chairperson Lina Khan, the Federal Trade Commission (FTC) has pursued more vigorous rulemaking and lowered the threshold for staff to launch investigations and sue companies. The Biden administration issued an executive order in July that empowered the FTC and the Department of Justice to more stringently enforce existing antitrust laws, challenge previous mergers, and create new rules addressing companies' accumulation of Americans' data. Separately, Google and Apple faced lawsuits over their app store fees, and a bundle of antitrust bills that could fundamentally reshape the US tech sector were introduced in Congress this year.

South Korea's Fair Trade Commission has been active over the past year. In August 2020, Apple paid \$84 million to settle an antitrust case after an investigation found that the company had abused its position of dominance by burdening local businesses with iPhone-related costs. In April 2021, the commission raided Facebook's local offices as part of a probe into whether the company forces app developers to advertise solely on its platform. And in June 2021, a new division was set up to investigate whether major companies like Facebook and Google have engaged in unfair practices, including the deceptive collection of personal data, to fuel online advertising.

In May 2021, Argentina's National Commission for the Defense of Competition ordered Facebook's WhatsApp platform to suspend the implementation of its new privacy policy for at least 180 days. The measure was part of an effort to ensure that the company does not "abuse its dominant market position," as the new policy would give Facebook access to users' data "at a level other companies

cannot replicate." Similar investigations into WhatsApp's privacy policy changes are underway in India.

Compelling platforms to share revenue with publishers

Regulators in several countries sought to pressure tech companies into negotiations with news publishers on the sharing of profits from advertising revenue. Google agreed in early 2021 to seek revenue-sharing agreements with French publishers in compliance with a new copyright law, but France's antitrust agency imposed a €500 million (\$600 million) fine in July on the grounds that the tech giant was not negotiating in good faith. In May 2021, Facebook agreed to share revenue with 14 Canadian publishers.

In Australia, a News Media Bargaining Code that was adopted in February 2021 raised tensions among major publishers, tech companies, and the government. The rules came about after the country's competition watchdog found that technology companies were not treating domestic media organizations fairly. The code establishes an arbitration regime requiring designated platforms to negotiate and pay a narrowly defined set of news outlets when their content is used. While competition policy can play a role in ensuring media diversity and sustainability, the Australian measure privileges legacy media institutions at the expense of newer, smaller, and more local outlets, and it does not stipulate that the beneficiaries must use the new revenue for journalistic purposes. The code also obliges platforms to share user data with media organizations, further embedding the news industry in the problematic targeted-advertising industry.

In response to the flawed legislation, Facebook took the extraordinary decision to block all news content for users based in Australia for one week. The move restricted access to community groups, health information, and other essential services in the process. Eventually, Facebook lifted the ban after the government made amendments to the code designed to extend revenue-sharing negotiations.

Competition policy as a tool for regime empowerment

In authoritarian states and other countries that lack effective due process guarantees, competition enforcement carries a stronger risk of abuse. Although monopolistic corporations and unfair market practices are just as corrosive to users' rights in such countries as they are in democracies, several cases demonstrate the potential for competition policy to

be enforced in an arbitrary or opaque manner that compels companies and prominent businesspeople to serve the leadership's political interests, granting the government greater control over the information space and access to sensitive data. For example, in April 2021, Russia's Federal Antimonopoly Service opened an investigation into allegations that Google was "abusing its dominant market position in video hosting services" at a time when the government was also demanding that YouTube, a Google subsidiary, remove content posted by opposition activists.

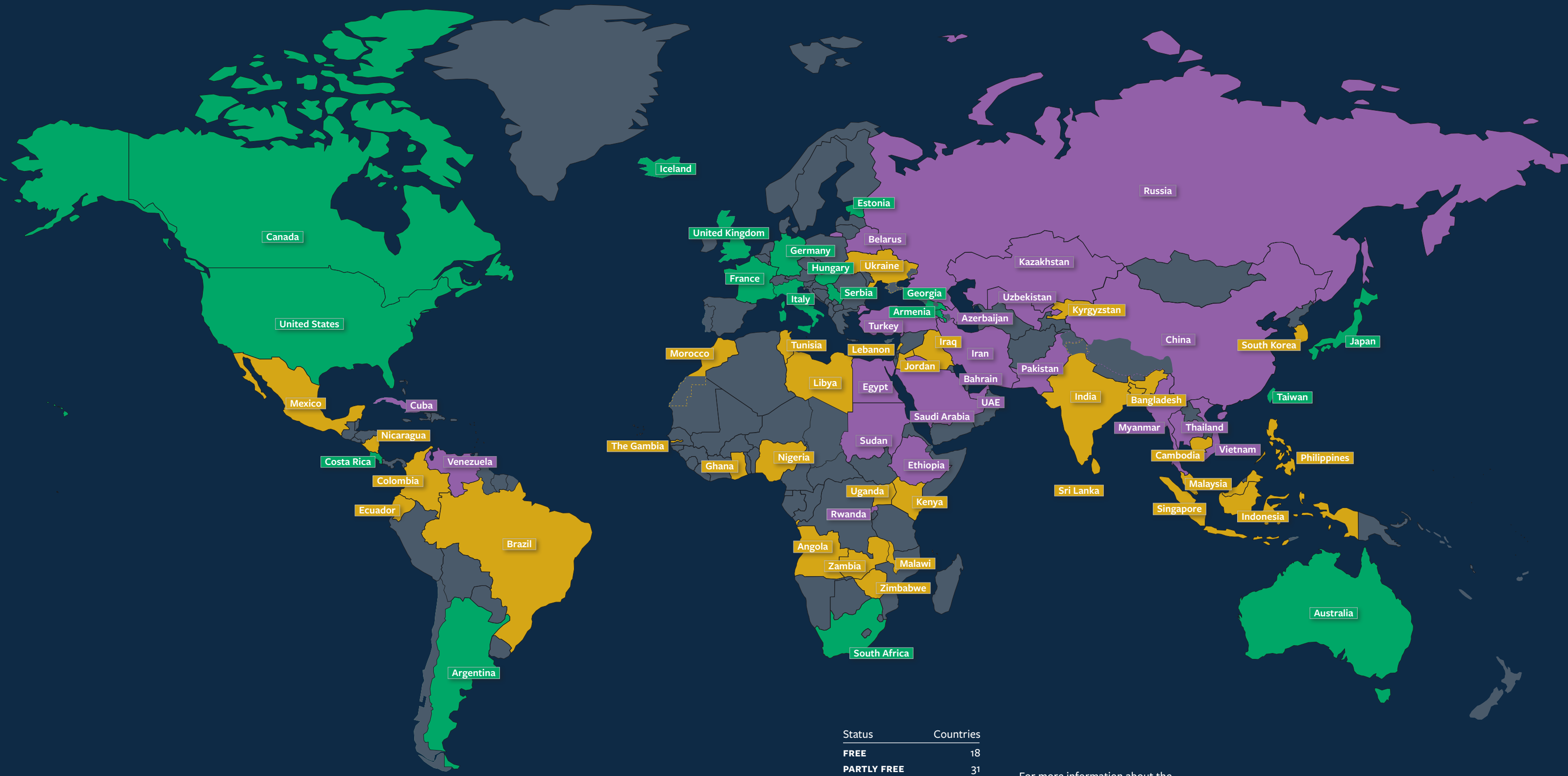
Chinese authorities have been among the most aggressive in addressing monopolistic practices and market abuses, though their interventions have raised concerns that the government is more interested in reining in these companies' autonomy and influence over the economy, public debate, and information space than in protecting the rights of citizens. New competition rules issued in February 2021 signaled the regime's unease with the rapid growth and consolidation of the country's tech sector. The regulations primarily target Alibaba and Tencent, with a specific focus on their respective financial services Alipay and WeChat Pay. The measures ban price fixing, predatory pricing, and the use of algorithms to manipulate the market. Two months later in April 2021, regulators slapped a record \$2.8 billion fine on Alibaba for using its algorithms and unfair access to data to further entrench its market position. Ant Group, an Alibaba affiliate and the parent company of Alipay, was also ordered to restructure into a financial holding company, putting it under stricter banking regulations. Alibaba was reportedly ordered to divest its media holdings, including stakes in the social media platform Weibo, due to the ruling Communist Party's concern that the company's influence over public opinion could rival its own.

The crackdown featured prominent signs of political motivation and direct pressure on business leaders. Alibaba founder Jack Ma had disappeared from public view for almost three months after contradicting senior government officials and criticizing regulators at an October 2020 conference. That November, a scheduled initial public offering for Ant Group was canceled, and an investigation into Alibaba's "monopolistic practices" was announced in December. Ma resurfaced in an online video ceremony in which he recited regime talking points about public welfare and rural revitalization.

Policies that ensure competition and limit concentrations of power among tech companies are crucial for ensuring a healthy democracy, but authoritarian states will continue to use such policies as a tool to reinforce their own unchecked authority.

Chinese authorities have been among the most aggressive in addressing monopolistic practices and market abuses, though their interventions have raised concerns that the government is more interested in reining in these companies' autonomy and influence.

FREEDOM ON THE NET 2021



FREE PARTLY FREE NOT FREE NOT ASSESSED

Status	Countries
FREE	18
PARTLY FREE	31
NOT FREE	21
Total	70

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

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 2020 to May 2021; cells with an asterisk (*) represent events that occurred between June and August 2021, when the report was sent to print. The Key Internet Controls reflect restrictions on content of political, social, or religious nature.

NO KEY INTERNET CONTROLS OBSERVED

	FOTN Score
Canada	87
Costa Rica	87
Estonia	94
France	78
Iceland	96
Japan	76
United Kingdom	78

Types of key internet controls

COUNTRY	Social media or communications platforms blocked	Political, social, or religious content blocked	ICT networks deliberately disrupted	Pro-government commentators manipulate online discussions	New law or directive increasing censorship or punishment passed	New law or directive restricting surveillance or increasing anonymity for blogger or ICT user arrested, imprisoned or in prolonged detention for political or social content	Blogger or ICT user physically attacked or killed (including in custody)	Technical attacks against government critics or human rights organizations	FOTN 2021 SCORE
Angola									62
Argentina									71
Armenia									71
Australia									75
Azerbaijan									35
Bahrain									30
Bangladesh									40
Belarus									31
Brazil									64
Cambodia									43
China									10
Colombia									65
Cuba									21
Ecuador					*				62
Egypt									26
Ethiopia						*			27
Georgia									77
Germany									79
Ghana									64
Hungary									70
India									49
Indonesia									48
Iran									16
Iraq									41
Italy									76
Jordan									47
Kazakhstan							*		33
Kenya									66
Kyrgyzstan									53
Lebanon									51
Libya									48
Malawi									59
Malaysia									58
Mexico									60
Morocco									53
Myanmar									17
Nicaragua									48
Nigeria									59
Pakistan									25
Philippines									65
Russia									30
Rwanda									38
Saudi Arabia									24
Serbia									71
Singapore									54
South Africa									73
South Korea									67
Sri Lanka									51
Sudan	*								33
Taiwan									80
Thailand									36
The Gambia									53
Tunisia									63
Turkey									34
Uganda									49
Ukraine									62
United Arab Emirates									27
United States									75
Uzbekistan									28
Venezuela									28
Vietnam					*				22
Zambia									59
Zimbabwe	*								46

June 2020 - May 2021 coverage period | 21 | 35 | 20 | 47 | 22 | 16 | 56 | 41 | 40 |

Recommendations

FOR POLICYMAKERS

Protect privacy and security

Strictly regulate the use of surveillance tools and the collection of personal information by government and law enforcement agencies. Government surveillance programs should adhere to the [International Principles on the Application of Human Rights to Communications Surveillance](#), a framework agreed upon by a broad consortium of civil society groups, industry leaders, and scholars for protecting users' rights. The principles, which state that all communications surveillance must be legal, necessary, and proportionate, should also be applied to open-source intelligence methods such as social media monitoring and biometric surveillance technologies. In the United States, lawmakers should reform or repeal existing surveillance laws and practices, including those under Section 702 of FISA and EO 12333—actions that may be necessary to secure data-sharing agreements with other democracies and the European Union. Policymakers should also investigate the extent to which commercial surveillance tools, such as spyware and extraction technology, have been used against Americans.

Enact robust data privacy legislation. Governments should enact updated legal frameworks that comprehensively safeguard user information. Individuals should have control over their information, including the right to access it, delete it, and easily transfer it to the providers of their choosing. Companies should be required to limit the collection of consumer data and disclose in plain language how they use it, as well as details on third parties that may access the data and how they are allowed to use it. Companies should be required to notify customers in a timely fashion if their information is compromised. Updated data privacy legislation should also provide a mechanism for independent verification of major foreign and domestic companies' data-collection practices to ensure compliance with local laws on privacy, nondiscrimination, and consumer protection. In the United States, lawmakers should pass a federal electronic privacy law that provides robust data protections, including for biometric data, and harmonizes rules among the 50 states. The Federal Trade Commission (FTC) and other relevant agencies should be empowered to pursue privacy enforcement using existing authorities.

Protect encryption. Policymakers should recognize that robust encryption is fundamental to cybersecurity, commerce, and human rights, and that weakening encryption endangers the lives of activists, journalists, members of marginalized communities, and ordinary users around the world. Governments should refrain from introducing legislation that mandates the introduction of so-called “back doors” or reduces intermediary liability protections for providers of end-to-end encryption services. In the United States, any reforms to Section 230 of the Communications Decency Act should not undermine the ability of intermediaries and service providers to offer robust encryption.

Restrict the export of censorship and surveillance technology. Democracies should place strict limits on the sale of technologies that enable monitoring, surveillance, interception, or collection of information and communications—including spyware, extraction technology, and systems whose machine learning, natural language processing, and artificial intelligence capabilities can be misused, and should consider new multilateral export controls. When reviewing export-licensing applications, governments should give extra scrutiny to applications from companies exporting products to countries [rated as Not Free or Partly Free by Freedom House](#). The most frequent abuses of censorship and surveillance occur in countries with these ratings. Businesses exporting technologies that could be used to commit human rights abuses should be required to report annually to the public 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 to ensure their products are not misused, human rights violations that have occurred as a result of the use or potential use of their technologies, and efforts to mitigate the harm done and prevent future abuses. Further, government export guidance should urge businesses to adhere to the [UN Guiding Principles on Business and Human Rights](#) when exporting dual-use technologies to countries rated Partly Free or Not Free by Freedom House. In the United States, Congress should pass the Foreign Advanced Technology Surveillance Accountability

Act, which requires the Department of State to include information on the status of surveillance and use of advanced technology in its annual report on global human rights practices. Specifically, the State Department must describe in each country report the extent of excessive surveillance and the use of advanced technology, such as facial recognition or biometric data collection, to impose (1) arbitrary or unlawful interference with privacy; or (2) unlawful or unnecessary restrictions on freedom of expression, peaceful assembly, association, or other internationally recognized human rights.

Guarantee competition, transparency, and accountability

Fully integrate human rights principles in competition policy enforcement. Strong competition in the digital market can encourage companies to create innovative products that protect fundamental freedoms and tackle online harms by empowering users to make informed choices about which products and platforms to use. When enforcing competition policy, regulators should consider the implications of market dominance on free expression, privacy, nondiscrimination, and other rights. Governments should also ensure antitrust frameworks can effectively be applied in the digital age, including by considering requirements for interoperability and data portability.

Enshrine human rights principles, transparency, and democratic oversight in laws that regulate online content.

Regulations addressing online content should establish special type- and size-oriented obligations on companies, incentivize platforms to improve their own standards, and require human rights due diligence and reporting. Such requirements should prioritize broad transparency across core products and practices, including content moderation, recommendation and algorithmic systems, collection and use of data, and targeted advertising practices. Intermediaries should continue to benefit from safe-harbor protections for most user-generated and third-party content appearing on their platforms, so as not to encourage restrictions that could inhibit free expression. Laws should also protect “good Samaritan” rules and reserve decisions on the legality of content for the judiciary rather than companies or executive agencies. Internet users whose content is removed should have access to adequate systems for notice, redress, and appeal. Moreover, independent, multistakeholder bodies with sufficient resources should be empowered to oversee laws’ implementation, conduct audits, and ensure compliance.

Foster a reliable and diverse information space

Maintain access to information and support free expression online, particularly during elections, protests, and periods of conflict.

Access to the internet is a human right. Intentional disruptions to internet access impact individuals’ economic, social, political, and civil rights. Governments should refrain from banning social media and messaging platforms. While such services may present genuine societal and national security concerns, bans constitute an arbitrary and disproportionate response that unduly restricts users’ cultural, social, and political speech. Governments should address any legitimate human rights or other risks posed by social media and messaging platforms through existing, democratic mechanisms—including regulatory action, security audits, parliamentary scrutiny, and legislation passed in consultation with civil society and affected stakeholders—rather than resorting to national security orders and emergency measures.

Address the digital divide. Unequal access to the internet entrenches societal inequity. In the short term, governments should work with service providers to lift data caps and waive fees for late payments; they should also support community-based initiatives to provide secure public access points and lend electronic devices to individuals who need them. Longer-term efforts should include expanding access and building internet infrastructure for underserved areas and populations, ensuring that connectivity is affordable, and enacting strong legal protections for user privacy and net neutrality. Governments should invest in digital literacy training through public education, public service advertising campaigns, and other mechanisms to target individuals from all age groups and socioeconomic backgrounds.

Protect global internet freedom

Elevate cyber diplomacy and coordination on global technology policy. Democracies should facilitate dialogue among national regulators and strengthen engagement at international standards-setting bodies. Diplomats should coordinate common approaches to countering authoritarian influence within the UN General Assembly, International Telecommunication Union (ITU), and other multilateral bodies. Multilateral decision-making should support but not replace specific internet-governance activities by nongovernmental or multistakeholder organizations. The United States should also push back against the increasing number of data localization requirements around the world. US lawmakers should pass legislation that elevates cyber policy within US foreign policy institutions, fosters greater cooperation among democratic allies, and establishes investment mechanisms for US technology in third countries, such as the Cyber Diplomacy Act (H.R.1251).

Prioritize defending and expanding internet freedom as a vital form of democracy, rights, and governance assistance. Recognizing the importance of internet freedom for the safety and efficacy of civil society around the world, governments should further resource digital security and digital activism trainings, and free software provision within existing democracy assistance programs. Governments should increase support for technologies that allow individuals in closed environments to circumvent government censorship, protect themselves against surveillance, and overcome temporary restrictions on connectivity. Such tools should be open-source, user-friendly, and locally responsive in order to ensure high levels of security and use.

FOR COMPANIES

Ensure fair and transparent content moderation. To ensure content moderation policies that are respectful of users, private companies should:

- Prioritize users' free expression and access to information, particularly for journalism; discussion of human rights; educational materials; and political, social, cultural, religious, and artistic expression.
- Clearly and completely explain in guidelines and terms of service what speech is not permissible, what aims such restrictions serve, and how the company assesses content.
- When appropriate, consider less invasive alternatives to content removal, such as labeling, fact-checking, adding context, promoting more authoritative sources, and implementing design changes that grant users more control over their information consumption.
- Ensure that content removal requests from governments comply with international human rights standards, and use all available channels to push back against problematic requests.
- Publish detailed transparency reports on content takedowns, both for those initiated by governments and for those undertaken by the companies themselves. Transparency reports should also address the use of automated and recommendation systems.
- Provide an efficient and timely avenue of appeal for users who believe that their rights were unduly restricted, including through censorship, banning, assignment of labels, or demonetization of posts.
- Refrain from relying on automated systems for flagging and removing content without opportunity for meaningful human review.
- Expand the capacity of content moderation teams by increasing their geographic and linguistic diversity, and conduct human rights due diligence assessments to ensure that implementation of moderation does not disproportionately affect marginalized communities.

Resist government orders to shut down internet connectivity or ban digital services. Service providers should use all available legal channels to challenge such requests from state agencies, whether they are official or informal. If companies cannot resist demands in full, they should ensure that any restrictions or disruptions are as limited as possible in duration, geographic scope, and type of content affected. Companies should also thoroughly document government demands internally and take steps to notify users as to why connectivity or content may be restricted, especially in countries where government actions lack transparency.

Adhere to the UN Guiding Principles on Business and Human Rights and conduct human rights impact assessments, with a commitment to do no harm. Companies should commit to respecting the 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 without judicial oversight, or provide surveillance or law enforcement equipment that is likely to be used to commit human rights violations. They should minimize the amount of data they collect, sell, and use, and clearly communicate to users what data are collected and for what purpose. International companies should not seek to operate in countries where they know they will be forced to violate international human rights principles. Where companies do operate, they should conduct periodic assessments to fully understand how their products and actions might affect rights including freedom of expression, nondiscrimination, and privacy. When a product is found to have been used for human rights violations, companies should suspend sales to the perpetrating party and develop an immediate action plan to mitigate harm and prevent further abuse. Companies should also mainstream end-to-end encryption in their products and ensure robust security protocols, including by resisting government requests to provide special decryption access.

Engage in continuous dialogue with civil society organizations to understand the implications of company policies and products. 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, managing government requests, and countering disinformation, among other activities.

FOR CIVIL SOCIETY

Conduct research on and raise awareness about censorship, surveillance, and content manipulation. Studies and surveys have shown that when users become more aware of censorship, surveillance, and disinformation, they often take actions that enhance internet freedom and protect fellow users. Civil society groups should engage in innovative initiatives that inform the public about government censorship and surveillance, as well as investigate and expose disinformation campaigns, including their origins and objectives.

Utilize strategic litigation to push back against shutdowns and censorship. Civil society groups and their allies have won victories in court that reversed network shutdowns and censorship decisions in Indonesia, India, Pakistan, Sudan, Togo, and Zimbabwe. They should participate in strategic litigation whenever possible, or provide friend-of-the-court filings that explain how certain forms or uses of digital technology undermine human rights. Civil society organizations should consider carefully whether to bring cases against governments themselves or support others seeking to do so, given that the process can be complicated and costly.

Work together with policymakers and the private sector to design and champion effective solutions. Some of the most important advances in privacy and free expression—such as the widespread adoption of end-to-end encryption and more secure communication via HTTPS browsing—derive from innovations in technical standards and product design that were advanced by advocacy groups. Multistakeholder efforts will be needed to ensure that leading democracies can offer a viable alternative to the authoritarian model of cyber sovereignty.

Methodology

WHAT WE MEASURE

The *Freedom on the Net* index measures each country's level of internet freedom based on a set of methodology questions. The methodology is developed in consultation with international experts to capture the vast array of relevant issues to human rights online (see "Checklist of Questions").

Freedom on the Net's core values are grounded in international human rights standards, particularly Article 19 of the Universal Declaration of Human Rights. The project particularly focuses on the free flow of information; the protection of free expression, access to information, and privacy rights; and freedom from both legal and extralegal repercussions arising from online activities. The project also evaluates to what extent a rights-enabling online environment is fostered in a particular country.

The index acknowledges that certain rights may be legitimately restricted. The standard of such restrictions within the methodology and scoring aligns with international human rights principles of necessity and proportionality, the rule of law, and other democratic safeguards. Censorship and surveillance policies and procedures should be transparent, minimal, and include avenues for appeal available to those affected, among other safeguards.

The project rates the real-world rights and freedoms enjoyed by individuals within each country. While internet freedom may be primarily affected by state behavior, actions by nonstate actors, including technology companies, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental. Over the years, *Freedom on the Net* has been continuously adapted to capture technological advances, shifting tactics of repression, and emerging threats to internet freedom.

THE RESEARCH AND SCORING PROCESS

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

1. **Obstacles to Access** details infrastructural, economic, and political barriers to access; government decisions to shut off connectivity or block specific applications or technologies; legal, regulatory, and ownership control over internet service providers; and the independence of regulatory bodies;
2. **Limits on Content** analyzes legal regulations on content; technical filtering and blocking of websites; other forms of censorship and self-censorship; the vibrancy and diversity of online information space; and the use of digital tools for civic mobilization;
3. **Violations of User Rights** tackles legal protections and restrictions on free expression; surveillance and privacy; and legal and extralegal repercussions for online speech and activities, such as imprisonment, cyberattacks, or extralegal harassment and physical violence.

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

Based on the score, Freedom House assigns the following internet freedom ratings:

- **Scores 100-70 = Free**
- **Scores 69-40 = Partly Free**
- **Scores 39-0 = Not Free**

Freedom House staff invite at least one researcher or organization to serve as the report author for each country, training them to assess internet freedom developments according to the project's comprehensive research methodology. Researchers submit draft country reports and attend a ratings review meeting focused on their region. During the meetings, participants review, critique, and adjust the draft scores—based on set coding guidelines—through careful consideration of events, laws, and practices relevant to each item. After completing the regional and country consultations, Freedom House staff edit and fact-check all country reports and perform a final review of all scores to ensure their comparative reliability and integrity. Freedom House staff also conduct robust qualitative analysis on every country to determine each year's key global findings and emerging trends.

Checklist of Questions

A. OBSTACLES TO ACCESS

(0–25 POINTS)

1. Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?

(0–6 points)

- Do individuals have access to high-speed internet services at their home, place of work, internet cafés, libraries, schools, and other venues, as well as on mobile devices?
- Does poor infrastructure (including unreliable electricity) or catastrophic damage to infrastructure (caused by events such as natural disasters or armed conflicts) limit residents' ability to access the internet?

2. Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons? (0–3 points)

- Do financial constraints—such as high prices for internet services, excessive taxes imposed on such services, or state manipulation of the relevant markets—make internet access prohibitively expensive for large segments of the population?
- Are there significant differences in internet penetration and access based on geographical area, or for certain ethnic, religious, gender, LGBT+, migrant, and other relevant groups?
- Do zero-rating plans or other pricing practices by service providers create a digital divide in terms of what types of content individuals with different financial means can access?

3. Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity? (0–6 points)

- Does the government restrict, or compel service providers to restrict, internet connectivity by slowing or shutting down internet connections during specific events (such as protests or elections), either locally or nationally?
- Does the government centralize internet infrastructure in a manner that could facilitate restrictions on connectivity?
- Does the government block, or compel service providers to block, social media platforms and communication apps that serve in practice as major conduits for online information?

- Does the government block, or compel service providers to block, certain protocols, ports, and functionalities within such platforms and apps (e.g., Voice-over-Internet-Protocol or VoIP, video streaming, multimedia messaging, Secure Sockets Layer or SSL), either permanently or during specific events?
 - Do restrictions on connectivity disproportionately affect marginalized communities, such as inhabitants of certain regions or those belonging to different ethnic, religious, gender, LGBT+, migrant, and other relevant groups?
- 4. Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers? (0–6 points)**
- Is there a legal or de facto monopoly on the provision of fixed-line, mobile, and public internet access?
 - Does the state place extensive legal, regulatory, or economic requirements on the establishment or operation of service providers?
 - Do licensing requirements, such as retaining customer data or preventing access to certain content, place an onerous financial burden on service providers?
- 5. Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner? (0–4 points)**
- Are there explicit legal guarantees that protect the independence and autonomy of any regulatory body overseeing the internet (exclusively or as part of a broader mandate) from political or commercial interference?
 - Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' legitimate interests?
 - Are decisions taken by regulatory bodies, particularly those relating to the internet, seen to be fair and to take meaningful notice of comments from stakeholders in society?
 - Are decisions taken by regulatory bodies seen to be apolitical and independent from changes in government?
 - Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?

B. LIMITS ON CONTENT

(0–35 POINTS)

- 1. Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards? (0–6 points)**
- Does the state use, or compel service providers to use, technical means to restrict freedom of opinion and expression, for example by blocking or filtering websites and online content featuring journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression?
 - Does the state use, or compel service providers to use, technical means to block or filter access to websites that may be socially or legally problematic (e.g., those related to gambling, pornography, copyright violations, illegal drugs) in lieu of more effective remedies, or in a manner that inflicts collateral damage on content and activities that are protected under international human rights standards?
 - Does the state block or order the blocking of entire social media platforms, communication apps, blog-hosting platforms, discussion forums, and other web domains for the purpose of censoring the content that appears on them?
 - Is there blocking of tools that enable users to bypass censorship?
 - Does the state procure, or compel services providers to procure, advanced technology to automate censorship or increase its scope?
- 2. Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards? (0–4 points)**
- Are administrative, judicial, or extralegal measures used to order the deletion of content from the internet, particularly journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression, either prior to or after its publication?

- Do digital platforms and content hosts arbitrarily remove such content due to informal or formal pressure from government officials or other powerful political actors?
 - Are access providers, content hosts, and third parties free from excessive or improper legal responsibility for opinions expressed by third parties transmitted via the technology they supply?
- 3. Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process? (0–4 points)**
- Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?
 - Are those that restrict content—including state authorities, ISPs, content hosts, digital platforms, and other intermediaries—transparent about what content is blocked or deleted?
 - Do efficient and timely avenues of appeal exist for those who find content they produced to have been subjected to censorship?
- 4. Do online journalists, commentators, and ordinary users practice self-censorship? (0–4 points)**
- Do internet users in the country engage in self-censorship on important political, social, or religious issues?
 - Are there unspoken rules that prevent users from expressing certain opinions via news sites, blogs, social media platforms, or private messages?
 - Do users avoid discussion of subjects that are likely to lead to retribution or result in censorship?
 - Do state surveillance or data collection practices have a chilling effect on online speech or cause users to avoid certain online activities of a civic nature?
 - Where widespread self-censorship exists, do some journalists, commentators, or ordinary users continue to test the boundaries, despite the potential repercussions?
- 5. Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest? (0–4 points)**
- Do government officials or other powerful actors pressure or coerce online news outlets, journalists, or bloggers to follow a particular editorial direction in their reporting and commentary?
 - Do authorities issue official guidelines or directives on coverage to online media outlets, including instructions to downplay or amplify certain comments or topics for discussion?
 - Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the content they produce or host?
 - Do government officials or other actors surreptitiously employ individuals or automated systems to artificially amplify political narratives or smear campaigns on social media?
 - Does disinformation, coordinated by foreign or domestic actors for political purposes, have a significant impact on public debate?
- 6. Are there economic, regulatory, or other constraints that negatively affect users' ability to publish content online? (0–3 points)**
- Are favorable informal connections with government officials necessary for online media outlets or service providers (e.g., search engines, email applications, blog-hosting platforms) to be economically viable?
 - Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it discourage advertisers from conducting business with disfavored online media or service providers?
 - Do onerous taxes, regulations, or licensing fees present an obstacle to participation in, establishment of, or management of online news outlets, blogs, or social media groups/channels?
 - Do ISPs manage network traffic and bandwidth availability in a manner that is transparent, is evenly applied, and does not discriminate against users or producers of content based on the nature or source of the content itself (i.e., do they respect “net neutrality” with regard to content)?
 - Does a lack of competition among content hosts and digital platforms limit users' ability to publish content online?
- 7. Does the online information landscape lack diversity and reliability? (0–4 points)**
- Are people able to access a range of local, regional, and international news sources that convey independent, balanced views in the main languages spoken in the country?

- Do online media outlets, social media pages, blogs, and websites represent diverse interests, experiences, and languages within society, for example by providing content produced by different ethnic, religious, gender, LGBT+, migrant, and other relevant groups?
 - Does the presence of misinformation undermine users' ability to access independent, credible, and diverse sources of information?
 - Does false or misleading content online significantly contribute to offline harms, such as harassment, property destruction, physical violence, or death?
 - If there is extensive censorship, do users employ virtual private networks (VPNs) and other circumvention tools to access a broader array of information sources?
- 8. Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues? (0–6 points)**
- Do online communities organize on political, social, cultural, and economic issues, including during electoral campaigns and nonviolent protests?
 - Do state or other actors limit access to online tools and websites (e.g., social media platforms, messaging groups, petition websites) for the purpose of restricting free assembly and association online?
 - Does the state place legal or other restrictions (e.g. criminal provisions, detentions, surveillance) for the purpose of restricting free assembly and association online?

C. VIOLATIONS OF USER RIGHTS

(0–40 POINTS)

- 1. Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence? (0–6 points)**
- Does the constitution contain language that provides for freedom of expression, access to information, and press freedom generally?
 - Are there laws or binding legal decisions that specifically protect online modes of expression?
 - Are online journalists and bloggers accorded strong rights and protections to perform their work?
 - Is the judiciary independent, and do senior judicial bodies and officials support free expression online?
 - Is there implicit impunity for private or state actors who commit crimes against online journalists, bloggers, or other people targeted for their online activities?
- 2. Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards? (0–4 points)**
- Do specific laws—including penal codes and those related to the media, defamation, cybercrime, cybersecurity, and terrorism—criminalize online expression and activities that are protected under international human rights standards (e.g., journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression)?
 - Are restrictions on internet freedom defined by law, narrowly circumscribed, and both necessary and proportionate to address a legitimate aim?
- 3. Are individuals penalized for online activities, particularly those that are protected under international human rights standards? (0–6 points)**
- Are writers, commentators, bloggers, or social media users subject to civil liability, imprisonment, arbitrary detention, police raids, or other legal sanction for publishing, sharing, or accessing material on the internet in contravention of international human rights standards?
 - Are penalties for defamation; spreading false information or “fake news”; national security, terrorism, and extremism; blasphemy; insulting state institutions and officials; or harming foreign relations applied unnecessarily and disproportionately?

4. Does the government place restrictions on anonymous communication or encryption? (0–4 points)

- Are website owners, bloggers, or users in general required to register with the government?
- Does the government require that individuals use their real names or register with the authorities when posting comments or purchasing electronic devices, such as mobile phones?
- Are users prohibited from using encryption services to protect their communications?
- Are there laws requiring that users or providers of encryption services turn over decryption keys to the government?

5. Does state surveillance of internet activities infringe on users' right to privacy? (0–6 points)

- Does the constitution, specific laws, or binding legal decisions protect against government intrusion into private lives?
- Do state authorities engage in the blanket collection of communications metadata and/or content transmitted within the country?
- Are there legal guidelines and independent oversight on the collection, retention, and inspection of surveillance data by state security agencies, and if so, do those guidelines adhere to international human rights standards regarding transparency, necessity, and proportionality?
- Do state authorities monitor publicly available information posted online (including on websites, blogs, social media, and other digital platforms), particularly for the purpose of deterring independent journalism or political, social, cultural, religious, and artistic expression?
- Do authorities have the technical capacity to regularly monitor or intercept the content of private communications, such as email and other private messages, including through spyware and extraction technology?
- Do local authorities such as police departments surveil residents (including through “stingray” technology), and if so, are such practices subject to rigorous guidelines and judicial oversight?
- Do state actors use artificial intelligence and other advanced technology for the purposes of online surveillance without appropriate oversight?
- Do government surveillance measures target or disproportionately affect dissidents, human rights defenders, journalists, or certain ethnic, religious, gender, LGBT+, migrant, and other relevant groups?

6. Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy? (0–6 points)

- Do specific laws or binding legal decisions enshrine the rights of users over personal data generated, collected, or processed by public or private entities?
- Can the government obtain user information from companies (e.g., service providers, providers of public access, internet cafés, social media platforms, email providers, device manufacturers) without a legal process?
- Are these companies required to collect and retain data about their users?
- Are these companies required to store users' data on servers located in the country, particularly data related to online activities and expression that are protected under international human rights standards (i.e., are there “data localization” requirements)?
- Do these companies monitor users and supply information about their digital activities to the government or other powerful actors (either through technical interception, data sharing, or other means)?
- Does the state attempt to impose similar requirements on these companies through less formal methods, such as codes of conduct, threats of censorship, or other economic or political consequences?
- Are government requests for user data from these companies transparent, and do companies have a realistic avenue for appeal, for example via independent courts?

7. Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities? (0–5 points)

- Are individuals subject to physical violence—such as murder, assault, torture, sexual violence, or enforced disappearance—in relation to their online activities, including membership in certain online communities?
- Are individuals subject to other intimidation and harassment—such as verbal threats, travel restrictions, nonconsensual sharing of intimate images, doxing, or property destruction or confiscation—in relation to their online activities?
- Are individuals subject to online intimidation and harassment specifically because they belong to a certain ethnic, religious, gender, LGBT+, migrant or other relevant group?

- Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such consequences?
- Have the online activities of dissidents, journalists, bloggers, human rights defenders, or other users based outside the country led to repercussions for their family members or associates based in the country?

8. Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack? (0–3 points)

- Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks meant to steal data or disable normal operations, including attacks that originate outside the country?
- Have websites belonging to opposition, news outlets, or civil society groups in the country been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?
- Are websites or blogs subject to targeted technical attacks as retribution for posting certain content, for example on political and social topics?
- Are laws and policies in place to prevent and protect against cyberattacks (including systematic attacks by domestic nonstate actors), and are they enforced?

Acknowledgements

Freedom on the Net is a collaborative effort between Freedom House staff and a network of more than 80 researchers, who come from civil society organizations, academia, journalism, and other backgrounds, covering 70 countries. In repressive environments, Freedom House takes care to ensure researchers' anonymity and/or works with experts living abroad.

This report was made possible by the generous support of Amazon, the Dutch Ministry of Foreign Affairs, Google, the Internet Society, the Lilly Endowment, the New York Community Trust, the U.S. State Department's Bureau of Democracy, Human Rights, and Labor (DRL), and Verizon. Freedom House is committed to editorial independence. Our donors do not influence the organization's research priorities, report findings, or policy recommendations.

CONTRIBUTORS

Freedom House staff

- [Adrian Shahbaz](#), Director, Technology and Democracy
- [Allie Funk](#), Senior Research Analyst, Technology and Democracy
- [Amy Slipowitz](#), Research Manager, *Freedom in the World*
- [Kian Vesteinsson](#), Research Analyst, Technology and Democracy
- Grant Baker, Research Associate, Technology and Democracy
- Cathryn Grothe, Research Associate
- Manisha Vepa, Research Associate
- Tessa Weal, Research Associate, Technology and Democracy

Elisha Aaron, David Meijer, Shannon O'Toole, and Tyler Roylance edited *Freedom on the Net*. Michael Abramowitz, Nicole Bibbins Sedaca, Annie Boyajian, Isabel Linzer, Sarah Repucci, Nate Schenckan, and Jennifer Stapleton provided valuable feedback on the summary of findings. Noah Buyon served as an adviser on Europe and Eurasia, while Sarah Cook and Angeli Datt served as advisers for China and Taiwan. Moosa Waraich provided research assistance.

Report authors

- **Argentina:** Eduardo Ferreyra, independent researcher
- **Armenia:** Samvel Martirosyan, co-founder of CyberHUB-AM
- **Australia:** Rose Dlougatch, lawyer
- **Azerbaijan:** Arzu Geybullayeva, Azerbaijan Internet Watch
- **Brazil:** Bruna Martins dos Santos, Advocacy Coordinator at Data Privacy Brazil Research
- **Cambodia:** Chak Sopheap, Cambodian Center for Human Rights
- **Canada:** Allen Mendelsohn, independent legal practitioner and McGill University Faculty of Law
- **Colombia:** Luisa Fernanda Isaza Ibarra, independent researcher
- **Costa Rica:** Luisa Ochoa Chaves, Freedom of Expression, Right to Information and Public Opinion Program (PROLEDI) and Communication Research Center (CICOM), University of Costa Rica (UCR); Giselle Boza Solano, PROLEDI UCR; Oscar Jimenez Alvarado, PROLEDI UCR
- **Cuba:** Ted A. Henken, Baruch College, City University of New York
- **Ecuador:** Iria Puyosa, Instituto de Investigaciones de la Comunicación
- **Estonia:** Hille Hinsberg and Kaspar Kala, Proud Engineers
- **Ethiopia:** Atnafu Brhane, Center for Advancement of Rights and Democracy
- **France:** Suzanne Vergnolle, postdoctoral researcher at Institut suisse de droit comparé
- **Georgia:** Teona Turashvili, Institute for Development of Freedom of Information
- **Germany:** Stina Lohmüller and Michael Puntschuh, iRights.Lab
- **Hungary:** Dalma Dojcsák, Hungarian Civil Liberties Union
- **Iceland:** Arnaldur Sigurðarson, independent researcher
- **Indonesia:** Sherly Haristya, independent researcher
- **Iran:** Melody Kazemi, Small Media
- **Iraq:** Hayder Hamzoz and Asia Abdulkareem, Iraqi Network for Social Media
- **Italy:** Philip Di Salvo, London School of Economics and Università della Svizzera italiana; Antonella Napolitano, Privacy International
- **Japan:** Hamada Tadahisa, Japan Computer Access for Empowerment

- **Jordan:** Issa Mahasneh, Jordan Open Source Association
- **Kazakhstan:** Adil Nurmakov, independent researcher; Yelzhan Kabyshev, director of Digital Paradigm Foundation
- **Lebanon:** Marianne Rahme, SMEX
- **Libya:** Muhammad Jaballa, independent researcher
- **Malawi:** Jimmy Kainja, University of Malawi
- **Malaysia:** Kelly Koh, Sinar Project
- **Mexico:** Mariel García-Montes, Massachusetts Institute of Technology
- **Myanmar:** Free Expression Myanmar
- **Nicaragua:** Abdías Zambrano, Gabriel Cajiga, and Marion Briancesco, IPANDETEC Central America
- **Nigeria:** 'Gbenga Sesan, Paradigm Initiative
- **Serbia:** Mila Bajić, Bojan Perkov, and Anka Kovačević, SHARE Foundation
- **Singapore:** Kirsten Han, independent researcher
- **South Africa:** Okyerebea Ampofo-Anti, Ampofo-Anti Consulting
- **South Korea:** Yenn Lee, SOAS University of London
- **Sri Lanka:** Raisa Wickrematunge, independent researcher
- **Sudan:** Reem Abbas, independent researcher and writer
- **Taiwan:** Ming-Syuan Ho, independent researcher
- **Thailand:** Emilie Pradichit, Manushya Foundation
- **The Gambia:** Demba Kandeh, University of The Gambia
- **Tunisia:** Yosr Jouini, independent researcher
- **Turkey:** Gürkan Özturan, Media Freedom Rapid Response Coordinator at the European Centre for Press and Media Freedom
- **Ukraine:** Olga Kyryliuk, independent legal practitioner and researcher
- **United Kingdom:** Aaron Ceross, University of Oxford
- **United States:** Alex Rochefort, Boston University
- **Uzbekistan:** Ernest Zhanaev, independent researcher
- **Venezuela:** Raisa Urribarri, Universidad de Los Andes (Emeritus)
- **Vietnam:** Trinh Huu Long, Legal Initiatives for Vietnam

Researchers for Angola, Bahrain, Bangladesh, Belarus, China, Egypt, Ghana, India, Kenya, Kyrgyzstan, Morocco, Pakistan, Philippines, Russia, Rwanda, Saudi Arabia, the United Arab Emirates, Uganda, Zambia, and Zimbabwe wished to remain anonymous.

Advisers

- Christopher Ali, Associate Professor for Department of Media Studies at the University of Virginia
- Endalkachew Chala, Hamline University
- Ernesto Falcon, independent researcher
- K Kabilan, independent researcher
- Ndesanjo Macha, independent researcher
- Alice E. Marwick, Associate Professor of Communication and Principal Researcher at the Center for Information, Technology, and Public Life at the University of North Carolina at Chapel Hill
- Bulanda T. Nkhowani, Program Officer, Southern Africa at Paradigm Initiative
- Lizzie O'Shea, Co-Founder and Chair, Digital Rights Watch Australia
- Riana Pfefferkorn, Stanford Internet Observatory
- Xiao Qiang, Founder and Editor-in-Chief of China Digital Times and research scientist at the School of Information, University of California Berkeley

The Freedom on the Net team expresses their gratitude to the global internet freedom community, including the many individuals and organizations whose tireless and courageous work informs this report.

HOW TO CITE THIS REPORT

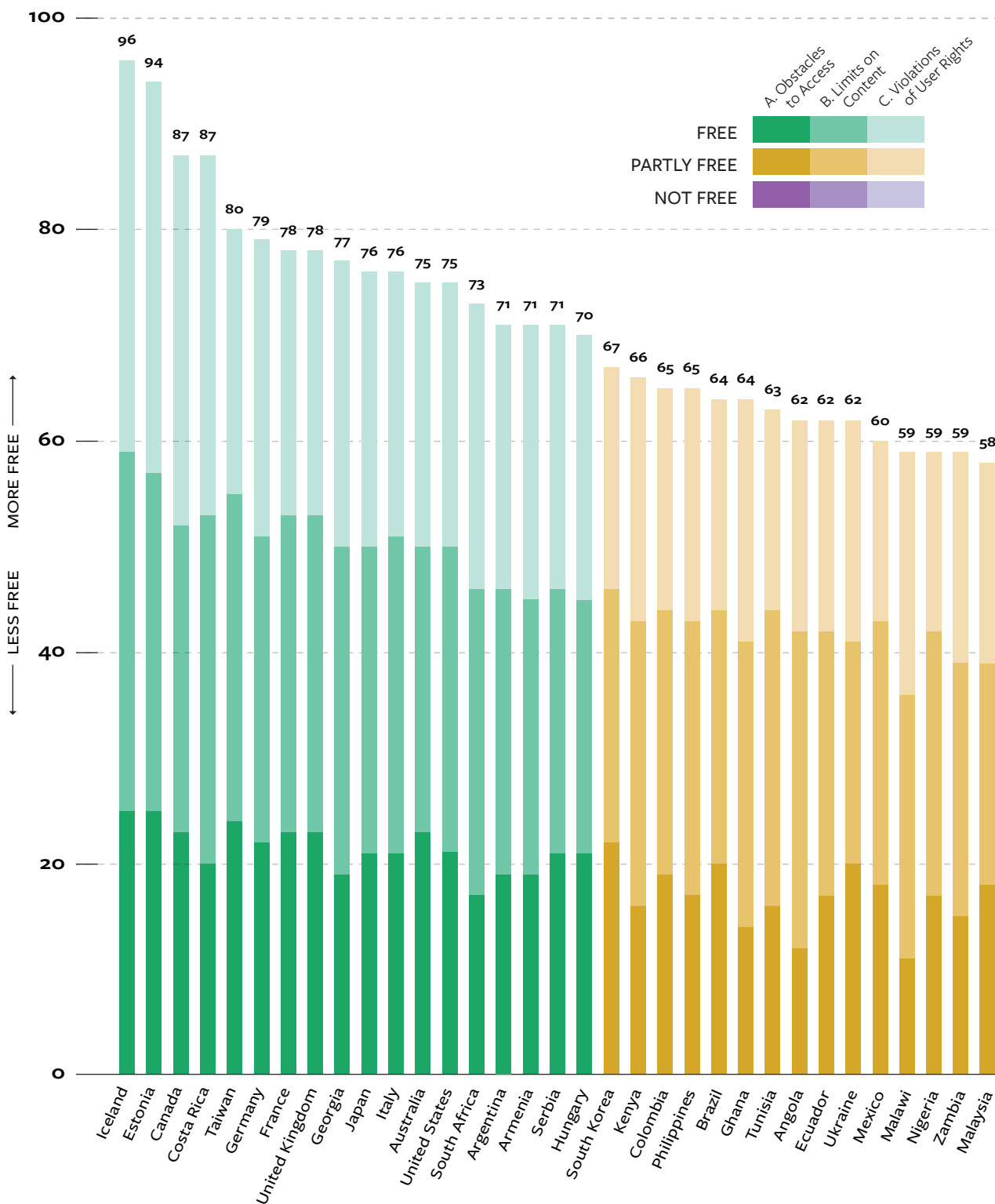
Shahbaz, Funk, Slipowitz, Vesteinsson, Baker, Grothe, Vepa, Weal eds. *Freedom on the Net 2021*, Freedom House, 2021, freedomonthenet.org.

Shahbaz and Funk, "The Global Drive to Control Big Tech," in Shahbaz, Funk, Slipowitz, Vesteinsson, Baker, Grothe, Vepa, Weal eds. *Freedom on the Net 2021*, Freedom House, 2021, freedomonthenet.org.

"Angola," in Shahbaz, Funk, Slipowitz, Vesteinsson, Baker, Grothe, Vepa, Weal eds. *Freedom on the Net 2021*, Freedom House, 2021, freedomonthenet.org.

GLOBAL RANKINGS

100 = Most Free 0 = Least Free



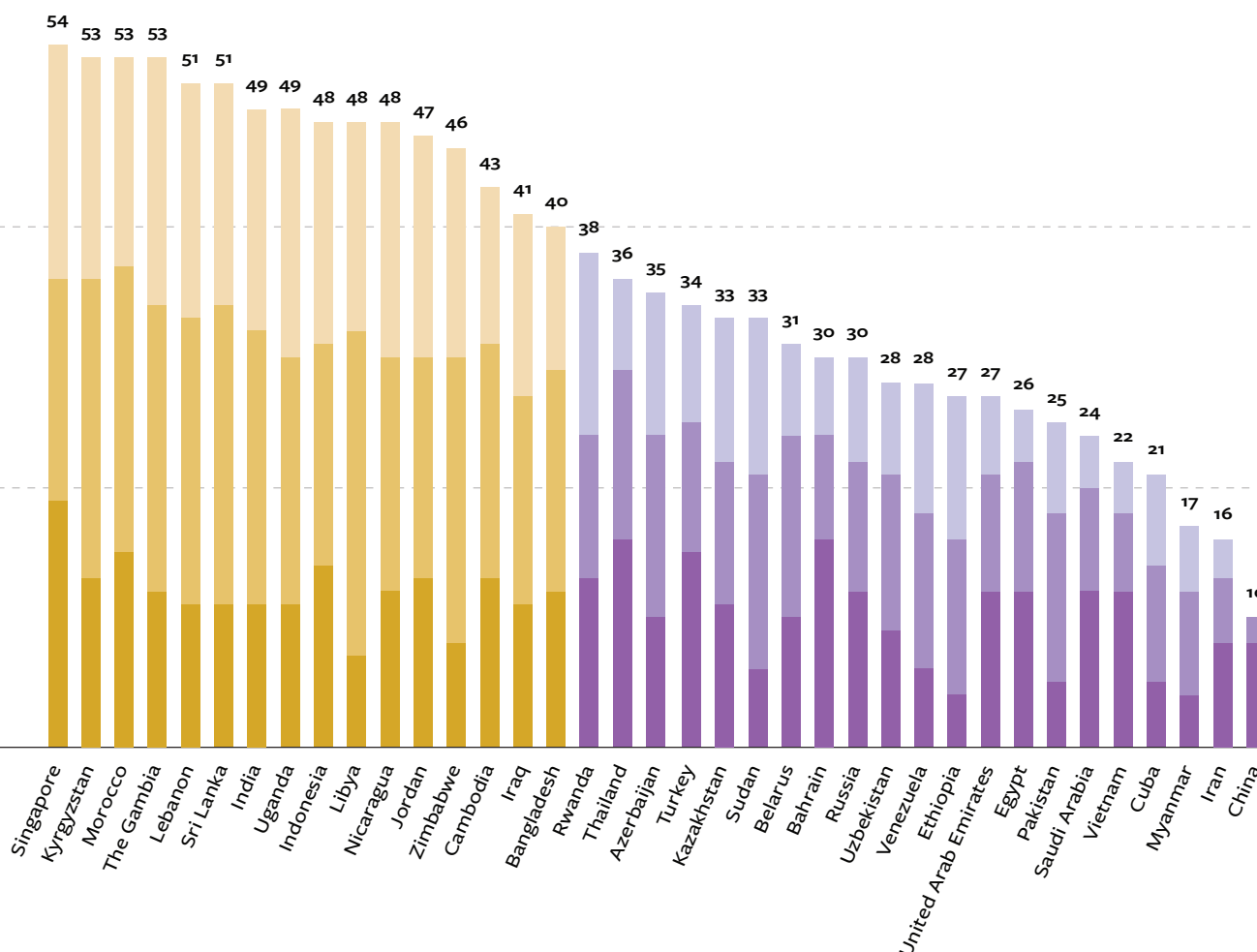
Freedom on the Net measures the level of internet freedom in 70 countries. Each country receives a numerical score from **100 (the most free)** to **0 (the least free)**, which serves as the basis for an internet freedom status designation of **FREE (100-70 points)**, **PARTLY FREE (69-40 points)**,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

Ratings are determined through an examination of three broad categories:

A. OBSTACLES TO ACCESS: Assesses infrastructural, economic, and political barriers to access; government decisions to shut off connectivity or block specific applications or technologies; legal, regulatory, and ownership control over internet service providers; and independence of regulatory bodies.

B. LIMITS ON CONTENT: Examines legal regulations on content; technical filtering and blocking of websites; other forms of censorship and self-censorship; the vibrancy and diversity of the online environment; and the use of digital tools for civic mobilization.

C. VIOLATIONS OF USER RIGHTS: Details legal protections and restrictions on free expression; surveillance and privacy; and legal and extralegal repercussions for online activities, such as prosecution, extralegal harassment and physical attacks, or cyberattacks.



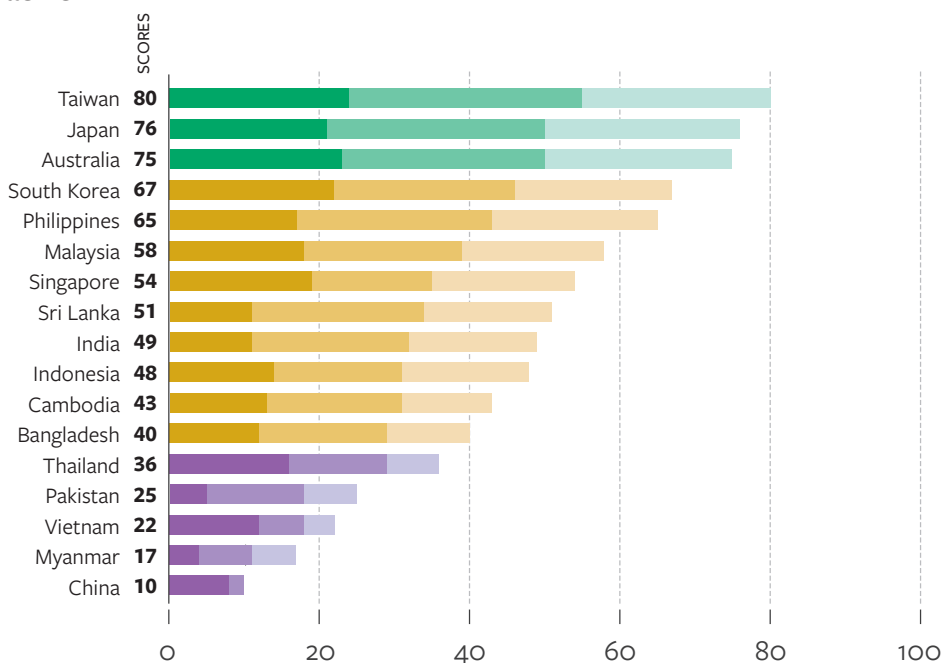
REGIONAL RANKINGS

Freedom on the Net 2021 covers 70 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

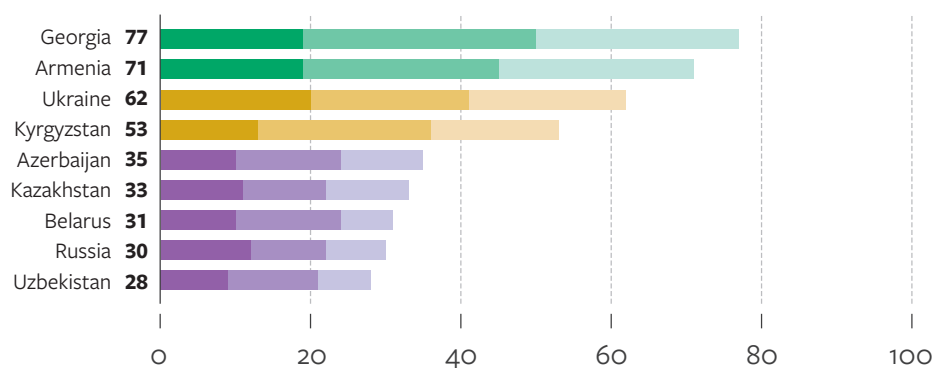
- A. Obstacles to Access
- B. Limits on Content
- C. Violations of User Rights



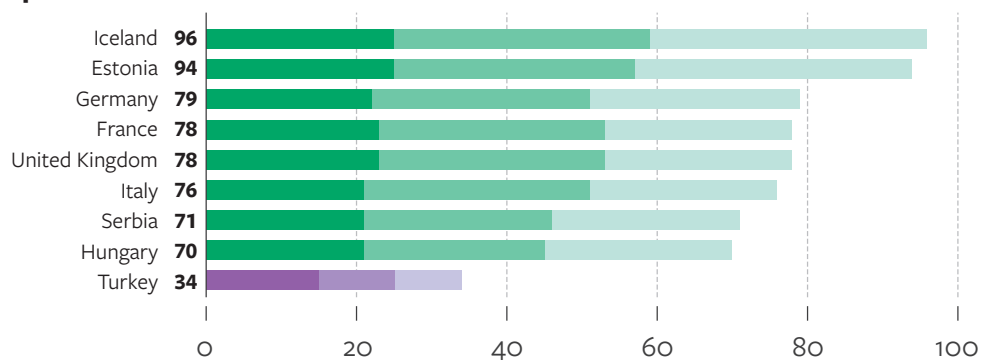
Asia-Pacific



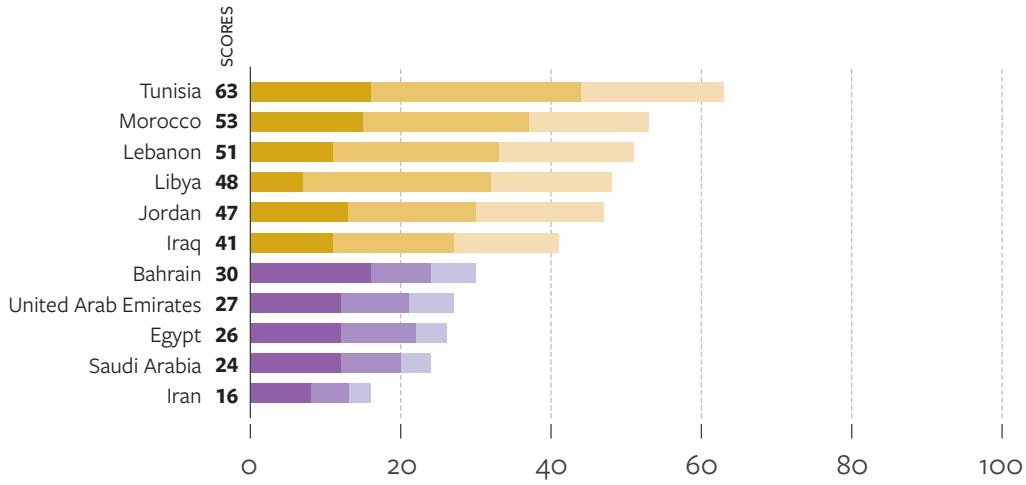
Eurasia



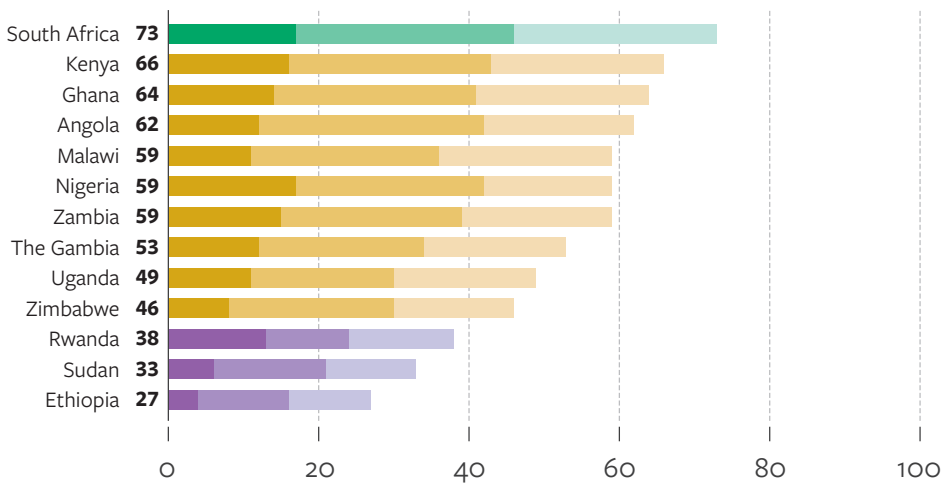
Europe



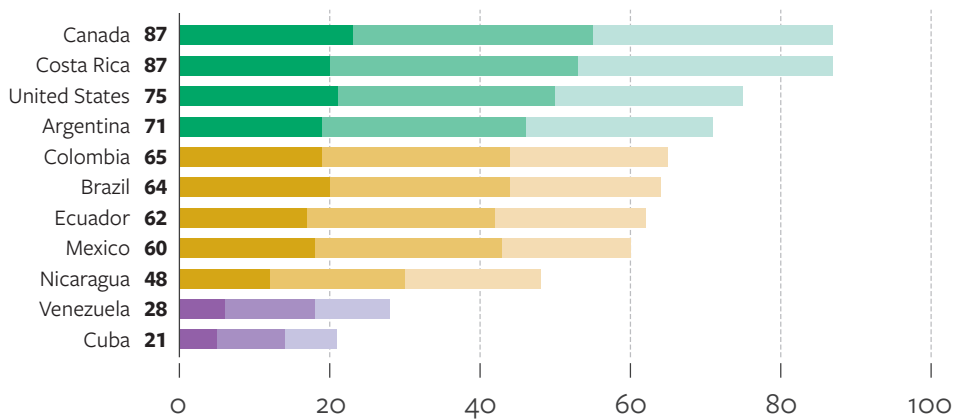
Middle East and North Africa



Sub-Saharan Africa



Americas



Board of Trustees

* Denotes members of the Executive Board

President

Michael J. Abramowitz

Chair

Michael Chertoff*

Vice Chair

Goli Ameri*

Peter Bass*

Treasurer

Robert Keane*

Secretary

Monde Muyangwa*

Trustees

Carol C. Adelman*

David E. Birenbaum

Sewell Chan

Jørgen Ejbøl*

Martin Etchevers

Francis Fukuyama

Jonathan Ginns

Dionisio Gutierrez

Rachel Kleinfeld

Jim Kolbe

Faith Morningstar

Sushma Palmer

Vivek Paul

Maurice A. Perkins

Andrew Prozes*

Ian Simmons

Thomas Staudt*

Robert H. Tuttle

Norman Willox*

We are proud to partner with individual philanthropists, foundations, corporations, NGOs, and governments who share our values and tireless pursuit of democracy and freedom. Join us in this critical work. For more information about supporting Freedom House, **please visit www.FreedomHouse.org/donate**.



Freedom House is a pro-democracy organization that identifies threats to freedom and mobilizes support for the activists and organizations that defend democracy. We strive to create a world where all people are free. This includes ensuring the United States champions democracy at home and abroad.

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

freedomhouse.org
facebook.com/FreedomHouseDC
[@freedomhouse](https://twitter.com/freedomhouse)
[@freedomonthenet](https://twitter.com/freedomonthenet)
202.296.5101
info@freedomhouse.org