Freedom House

FREEDOM ON THE NET 2020

The Pandemic's Digital Shadow

FREEDOM ON THE NET 2020

TABLE OF CONTENTS

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

The following people were instrumental in the research and writing of this report: Noah Buyon, Cathryn Grothe, Amy Slipowitz, and Kian Vesteinsson. Michael Abramowitz, Annie Boyajian, Arch Puddington, Sarah Repucci, Nate Schenkkan, Jennifer Stapleton, and Mai Truong provided valuable feedback on the summary of findings. Elisha Aaron, David Meijer, Shannon O'Toole, and Tyler Roylance edited the report. Isabel Linzer and Sarah Cook served as advisers on Sub-Saharan Africa and China, respectively. Ever Bussey and Maddie Masinsin provided research assistance.

This booklet is a summary of findings for the 2020 edition of Freedom on the Net. Narrative reports on the 65 countries assessed in this study and a full list of contributors can be found on our website at **freedomonthenet.org**.

ON THE COVER

A young woman wearing a protective mask looks at her smartphone while passing by graffiti representing two big watching eyes in Berlin, Germany on April 1, 2020. Illustrative Editorial (Photo by Emmanuele Contini/NurPhoto via Getty Images)

Freedom House

The Pandemic's Digital Shadow

by Adrian Shahbaz and Allie Funk

The coronavirus pandemic is accelerating a dramatic decline in global internet freedom. For the 10th consecutive year, users have experienced an overall deterioration in their rights, and the phenomenon is contributing to a broader crisis for democracy worldwide.

In the COVID-19 era, connectivity is not a convenience, but a necessity. Virtually all human activities—commerce, education, health care, politics, socializing—seem to have moved online. But the digital world presents distinct challenges for human rights and democratic governance. State and nonstate actors in many countries are now exploiting opportunities created by the pandemic to shape online narratives, censor critical speech, and build new technological systems of social control.

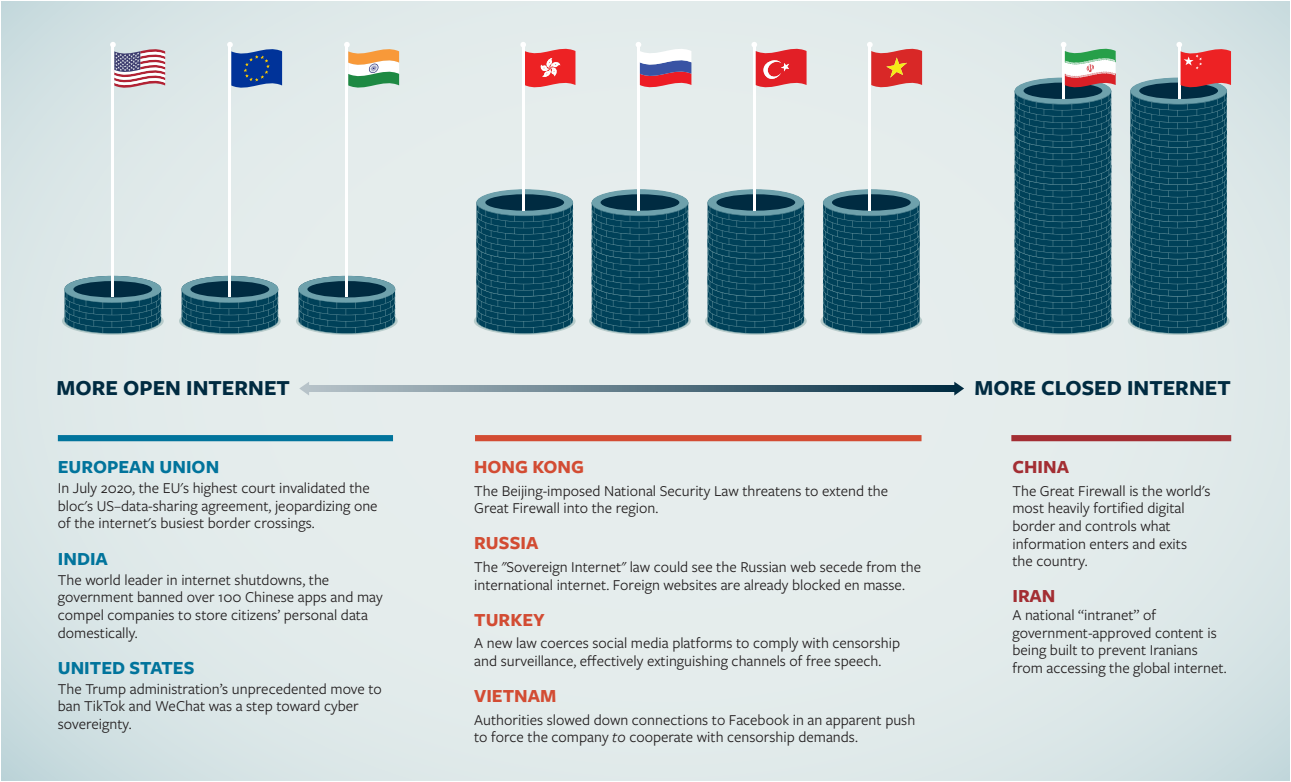
Three notable trends punctuated an especially dismal year for internet freedom. First, political leaders used the pandemic as a pretext to limit access to information. Authorities often blocked independent news sites and arrested individuals on spurious charges of spreading false news. In many places, it was state officials and their zealous supporters who actually disseminated false and misleading information with the aim of drowning out accurate content, distracting the public from ineffective policy responses, and scapegoating certain ethnic and religious communities. Some states shut off connectivity for marginalized groups, extending and deepening existing digital divides. In short, governments around the world failed in their obligation to promote a vibrant and reliable online public sphere.

Second, authorities cited COVID-19 to justify expanded surveillance powers and the deployment of new technologies that were once seen as too intrusive. The public health crisis has created an opening for the digitization, collection, and analysis of people's most intimate data without adequate protections against abuses. Governments and private entities are ramping up their use of artificial intelligence (AI), biometric surveillance, and big-data tools to make decisions that affect individuals' economic, social, and political rights. Crucially, the processes involved have often lacked transparency,

State and nonstate actors are exploiting opportunities created by the pandemic to shape online narratives, censor critical speech, and build new technological systems of social control.

RISING CYBER SOVEREIGNTY THREATENS TO FURTHER SPLINTER THE INTERNET

More governments are imposing restrictions on the flow of information across national borders.



independent oversight, and avenues for redress. These practices raise the prospect of a dystopian future in which private companies, security agencies, and cybercriminals enjoy easy access not only to sensitive information about the places we visit and the items we purchase, but also to our medical histories, facial and voice patterns, and even our genetic codes.

The third trend has been the transformation of a slow-motion "splintering" of the internet into an all-out race toward "cyber sovereignty," with each government imposing its own internet regulations in a manner that restricts the flow of information across national borders. For most of the period since the internet's inception, business, civil society, and government stakeholders have participated in a consensus-driven process to harmonize technical protocols, security standards, and commercial regulation around the world. This approach allowed for the connection of billions of people to a global network of information and services, with immeasurable benefits for human development, including new ways to hold powerful actors to account.

> Countries across the democratic spectrum are erecting their own digital borders in a sign of fraying trust in the open internet.

The allure of cyber sovereignty

Rather than protecting users, the application of national sovereignty to cyberspace has given authorities free rein to crack down on human rights while ignoring objections from local civil society and the international community. China's regime, a pioneer in this field and the world's worst abuser of internet freedom for the sixth year in a row, has long blocked popular foreign services and centralized technical infrastructure to allow for the pervasive monitoring and filtering of all traffic coming into the country. Following this model, Russian

A Kashmiri journalist holds a placard at the Kashmir Press Club during a protest against connectivity restrictions imposed since August 2019. Photo credit: Muzamil Mattoo/NurPhoto via Getty Images.

authorities have passed legislation to isolate the country from the international internet during national emergencies, and Iran's government similarly cut off connections to hide the police's violent response to mass protests in late 2019.

Recent events in Hong Kong illustrate in frightening detail the implications of greater state control over the online civic space. The leadership in Beijing directly imposed a draconian National Security Law on the autonomous region, prescribing harsh punishments for broadly defined speech offenses that encompass any expressions of solidarity with prodemocracy protesters. To escape such penalties, political websites, online forums, personal social media accounts, and entire apps engaged in preemptive closures or deletions. At the same time, US technology companies announced that they would suspend data-sharing agreements with local law enforcement officials to avoid complicity in human rights abuses. Authorities could raise the cost of noncompliance by mandating that companies store user data within the jurisdiction or face blocking, large fines, or the arrest of company representatives.

Alarmingly, these sorts of practices are not unique to the world's most repressive regimes. Countries across the democratic spectrum are erecting their own digital borders in a sign of fraying trust in the open internet. The United States and India banned many popular Chinese apps, citing national security concerns. Legislators in Brazil, Nigeria, and Turkey passed or considered regulations requiring companies to keep user data from leaving the country, meaning law enforcement agencies would have easier access to sensitive information. The European Union's highest court found that US national security programs violate Europeans' privacy rights, invalidating one of the world's largest data-sharing agreements. Even when aimed at curbing repressive practices, these actions serve to legitimize the push for each state to oversee its own "national internet," which was previously championed only by autocratic governments in countries such as China, Iran, and Russia.

A stronger role for global civil society

The best way to stave off the rise of cyber sovereignty is to restore confidence in the legitimacy and efficacy of the existing multistakeholder model. This means envisioning new systems of internet and platform governance that uphold democratic principles of popular representation and participation. Current self-regulatory mechanisms run into difficulties when the public interest contrasts with the self-interest of the tech industry. While the scale of the international discussion—and of the leading platforms themselves—makes it difficult to incorporate input from all members of the public, global civil society organizations can provide the expertise and independent oversight required to tackle some of the problems surrounding the impact of technology on human rights.

Future initiatives on platform governance and content moderation should go beyond mere transparency. They will have to ensure that systemic human rights deficiencies flagged by various independent assessments are addressed and replaced with updated rights-respecting practices and policies for the entire internet and telecommunications industry.

As COVID-19 has demonstrated, addressing the challenges of an interconnected world requires effective coordination among policymakers and civil society from all countries. For matters related to competition, taxation, and cross-border data flows, for example, intergovernmental coordination is likely to prove more effective than ad hoc state regulation, due to the internet's

Addressing the challenges of an interconnected world requires effective coordination among policymakers and civil society from all countries.

global nature. New institutions built for the digital age can manage transnational problems that do not fall neatly under one government's jurisdiction, while ensuring that users in smaller or less powerful countries receive the same protections and care as their counterparts in large democracies. This international, multistakeholder approach will not halt the efforts of the Chinese and Russian governments to fortify themselves against—and impose their will on—the global network, but it may limit short-sighted regulatory initiatives by established and aspiring democracies, preventing a further splintering of the internet.

An irreplaceable asset for democracy

There is tremendous value to an internet that is open, free, and global. Even in settings that are otherwise highly oppressive, an unrestricted online space offers immeasurable possibilities for free expression, community engagement, and economic development.

But when civic organizing and political dissent overflow from the realm of social media onto the streets of cities like Minsk, Khartoum, and Caracas, dictators shut down networks to choke off any calls for greater democracy and human rights. State and nonstate actors drown out political dissent by spreading fear and disinformation on online platforms, even resorting to arrests and physical intimidation in some cases. Protesters from Hong Kong to Minneapolis—equipped with cameras and the courage of their convictions—risk retribution from the world's most technologically advanced security forces.

If digital communication platforms are to advance the cause of human rights in the 21st century, the internet freedom movement must raise its ambitions from simply demanding policies that respect basic rights, to actually building robust governance structures that enshrine and enforce those protections. This report outlines concrete recommendations for governments, technology companies, and civil society on how to rekindle faith in a free internet and push back against digital authoritarianism and repressive cyber sovereignty. Reversing the antidemocratic transformation of today's internet is a vital step in preventing even worse outcomes that could arise from the digital technologies of tomorrow.

GLOBAL INTERNET USER STATS

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

According to Freedom House estimates:

73% live in countries where individuals were arrested or imprisoned for posting content on political, social, or religious issues.

64% live in countries where individuals have been attacked or killed for their online activities since June 2019.

61% 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.

47% live in countries where authorities disconnected internet or mobile networks, often for political reasons.

34% live in countries where access to social media platforms was temporarily or permanently restricted.

Tracking the Global Decline

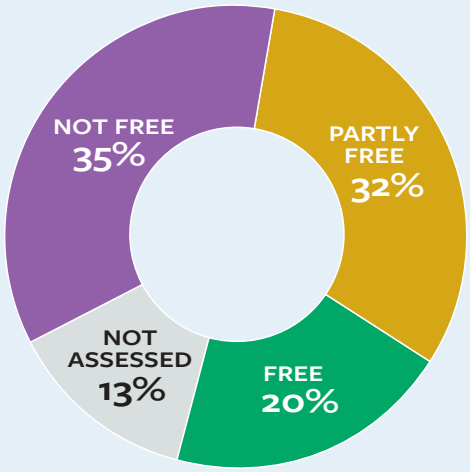
A rundown of prominent changes to countries' internet freedom scores

Global internet freedom has declined for the 10th consecutive year: 26 countries' scores worsened during this year's coverage period, while 23 countries registered net gains. The largest declines occurred in Myanmar and Kyrgyzstan, followed by India, Ecuador, and Nigeria. A record number of countries featured deliberate disruptions to internet service. On the positive side, Sudan and Ukraine experienced the largest improvements, followed by Zimbabwe. A raft of court rulings shored up human rights online in countries ranked Free, Partly Free, and Not Free alike. The United States ranked seventh overall, while Iceland was once again the top performer. For the sixth consecutive year, China was found to have the worst conditions for internet freedom.

Freedom on the Net assesses internet freedom in 65 countries around the globe, accounting for 87 percent of the world's internet users. This report, the 10th in its series, covers developments between June 2019 and May 2020. More than 70 analysts contributed to this year's report, using a standard methodology to determine each country's internet freedom score on a 100-point scale, based on 21 indicators pertaining to obstacles to access, limits on content, and violations of user rights. *Freedom on the Net* also identifies global trends related to the impact of information and communication technologies on democracy. The data underpinning this year's trends, in-depth reports on each of the countries surveyed, and the full methodology can be found at freedomonthenet.org.

GLOBAL INTERNET POPULATION BY 2020 FOTN STATUS

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



Countries in decline

Myanmar's internet freedom score fell by five points, as a government-ordered internet blackout has left some 1.4 million people living in Rakhine and Chin States without access almost continuously since June 2019. The government also blocked several independent news outlets and sites serving ethnic minority groups, some of which were reporting on the military's human rights abuses against the Rohingya and other groups. At the same time, online content inciting violence against the Rohingya and other marginalized groups proliferated on the Burmese internet.

Internet freedom in Kyrgyzstan declined by five points as well. In August 2019, the government briefly disrupted connectivity in Koi-Tash, where supporters of former president Almazbek Atambayev clashed violently with special forces sent to arrest him. Investigative journalists who exposed a far-reaching corruption ring were targeted with punitive defamation lawsuits and roughed up by unknown assailants, and their websites were disabled by distributed denial-of-service (DDoS) attacks. Police also embarked on a campaign against rumors related to the COVID-19 pandemic, detaining people who purportedly spread false news and in some cases forcing them to publicly apologize.

India lost four points. The world's largest democracy remains the world leader in internet shutdowns; last year, for the first time, the government disrupted connectivity in major cities, a milestone occasioned by demonstrations against a discriminatory law that gave certain non-Muslim groups special access to citizenship. Authorities increasingly pressured social media companies such as Twitter and

streaming platforms like Netflix to remove content that was critical of the government's Hindu nationalist agenda and its actions in Jammu and Kashmir, India's only Muslim-majority state until it was stripped of its semiautonomous status and divided into two "union territories" in 2019. In addition, new evidence pointed to the use of spyware against prominent activists, journalists, and lawyers involved in advocating for the rights of marginalized groups.

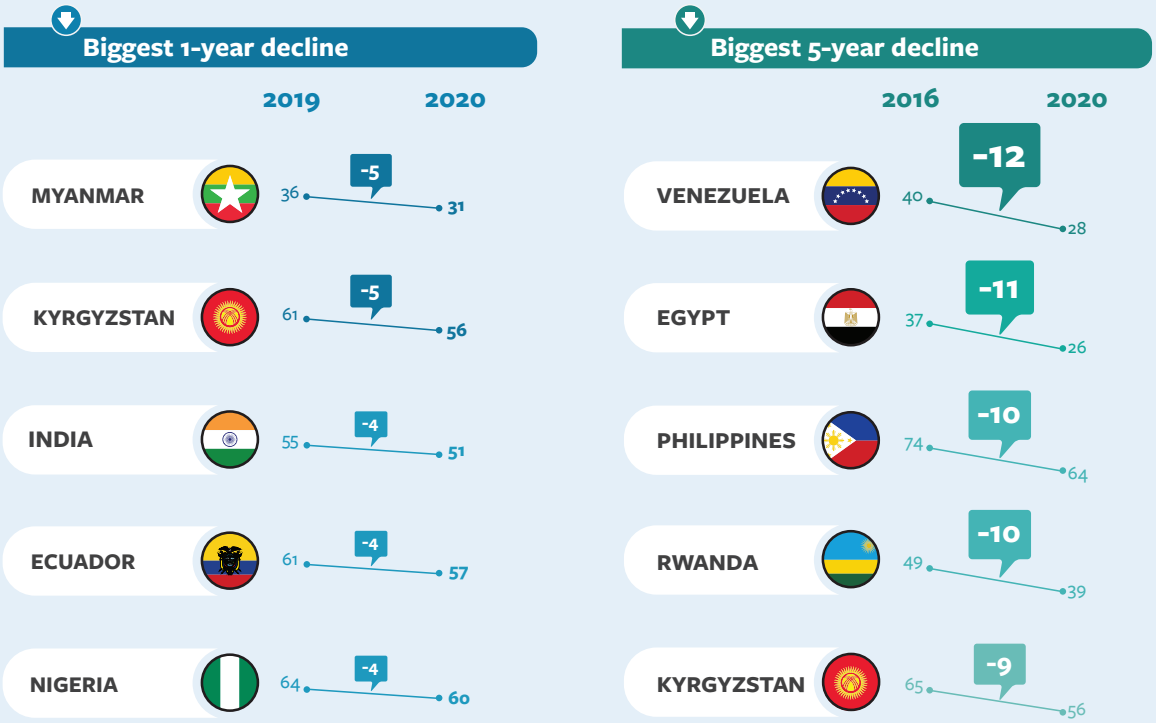
Ecuador saw its overall score decline by four points after austerity measures that were ordered in October 2019 sparked mass protests. The demonstrations were met with intentional, targeted disruptions to internet connections as well as to Facebook and WhatsApp's image-sharing functionalities, preventing protesters from communicating with one another and journalists from carrying out their work. Separately, online journalists who investigated local politicians and criminal groups continued to experience violence and death threats, with one journalist targeted in a bombing at his home.

Internet freedom in Nigeria also declined, as the government tightened its grip on the online media environment. Journalists and outlets experienced cyberattacks—some allegedly linked to security forces—and police used call records obtained from service providers to arrest reporters. However, a few websites that were previously blocked under government orders are now accessible, and Nigerians remain active in their use of social media to call for political and social change.

Score declines in Rwanda caused the country to fall from Partly Free to Not Free, and new evidence suggested that the government uses sophisticated spyware to monitor and intimidate exiled dissidents. In addition, the country's

LARGEST ONE-YEAR AND FIVE-YEAR SCORE DECLINES

Of the 65 countries covered by *Freedom on the Net*, these experienced the steepest one-year and five-year declines in internet freedom.



Senate released a report that smeared news outlets and opposition figures with allegations of genocide denial; those targeted subsequently experienced censorship and harassment. Over a dozen bloggers and journalists were arrested during the country's strict COVID-19 lockdown.

More broadly, this year *Freedom on the Net* observed intentional disruptions to connectivity in a record 22 out of 65 countries. Many of these disruptions, including Iran's November 2019 countrywide blackout and shutdowns in Moscow in August and September 2019, were directly precipitated by protests. Such practices are an ultimate expression of contempt for freedoms of association and assembly, as well as for the right to access information.

Cautious improvements

Sudan's internet freedom score improved by five points under a transitional government that was formed by military commanders and civilian protest leaders to replace the repressive regime of longtime president Omar al-Bashir. The interim constitution contains language that protects freedom of expression and access to the internet. However, optimism about the country's trajectory was tempered by renewed connectivity restrictions at the beginning and end of the coverage period, including a 40-day shutdown following a brutal massacre of protesters by security forces in June 2019.

Ukraine's five-point improvement also comes with caveats. For the first time, *Freedom on the Net* excluded the occupied regions of eastern Ukraine from its assessment in order to align the survey with Freedom House's *Freedom in the World* report, which assesses conditions in the Eastern Donbas area separately because they are so different from those in government-controlled Ukraine. As a result of this methodological change, Ukraine's score improved. However, the new administration of President Volodymyr Zelenskyy also presided over more tangible improvements, such as the removal of telecommunications licensing requirements that have historically been associated with corruption. It largely abandoned the previous practices of administratively blocking websites—although in a disappointing May 2020 move, Zelenskyy extended sanctions on several Russian-owned technology companies.

Zimbabwe registered a four-point improvement, in part because there was no repetition of the connectivity restrictions the government had imposed during a violent crackdown on protests in January 2019. However, the authorities continued to arrest and harass internet users who shared critical commentary, with security forces going so far as to abduct and torture an online comedian. A two-day internet shutdown during anticorruption protests after the coverage period similarly suggested that the score improvement may be short-lived.

Courts upheld protections for human rights online in several countries across the democratic spectrum, issuing landmark decisions on the illegitimacy of internet shutdowns, online censorship, and bulk surveillance. In June 2019, a court in Sudan ordered an end to that country's weeks-long internet shutdown; a year later, judges in Indonesia found that government-imposed shutdowns amid protests in Papua and West Papua Provinces were illegal. Litigation in Pakistan led a court to denounce an arbitrary website blocking as a violation of due process, while Georgia's constitutional court invalidated a regulation on "inadmissible content" whose broadly worded prohibitions threatened the viability of media outlets and internet service providers. Meanwhile, judges in Brazil, Estonia, Germany, and South Africa moved to limit state surveillance powers. Taken together, these rulings show that courts—when acting fairly and independently—can serve as powerful defenders of internet freedom.

Contrasting models for internet policy

China ranked last in *Freedom on the Net's* analysis for the sixth consecutive year. New content controls and user arrests were reported throughout the coverage period, including in connection with speech about the Hong Kong protest movement that emerged in mid-2019. With the onset of COVID-19, every component of the regime's internet control apparatus—including automated censorship, high-tech surveillance, and large-scale arrests—was activated to stanch the spread of not just the virus but also unofficial information and criticism of the government. State officials and media, backed by bots and trolls, promoted disinformation domestically and in targeted campaigns around the world. Nevertheless, some creative and courageous users in China managed to share important details about the first days of the outbreak and

the lockdown with the international community, while also circulating and archiving investigative reporting.

Iceland remained the most steadfast protector of internet freedom, with high rates of access, few restrictions on content, and strong safeguards for human rights online. These rights were expanded with the passage of a whistleblower-protection law during the coverage period, though other long-awaited reforms on issues such as intermediary liability remain stalled in the parliament.

The failings of internet freedom's traditional champion

Internet freedom dropped by one point in the United States, which has now experienced four consecutive years of decline. Even as Facebook, Twitter, and other social media platforms were used to great effect to organize civic activism like the Black Lives Matter protests, growing surveillance of social media by federal and local law enforcement agencies undermined these tools' usefulness, especially after several people experienced targeted harassment and even spurious criminal charges for their posts or retweets. The coverage period also saw the online sphere flooded with politicized disinformation and harmful misinformation related to both the protests and COVID-19. While it did not contribute to the year's score change, this deluge highlighted a collective failure to address content manipulation—homegrown or otherwise—since the 2016 election first thrust the phenomenon into the spotlight. It also boded ill for the upcoming 2020 election.

An executive order signed by President Donald Trump in May marked a shift away from the robust intermediary-liability protections that have long been synonymous with the US internet freedom model. After the coverage period, the president ordered US individuals and entities to halt transactions with TikTok and WeChat, potentially forcing the popular Chinese-owned social media platforms to sell or abandon US operations that have an estimated 50 million and 19 million users, respectively. The parent companies of WeChat and TikTok are based in mainland China, where firms regularly comply with government demands to censor content, manipulate discussions, and share user data with Chinese state security agencies, leading some experts to warn that the apps present a threat to US national security.

The new policies adopted by Washington constitute an arbitrary and disproportionate response to the genuine risks posed by the apps, particularly in the absence of strong data-privacy legislation that outlines the standards Americans should expect from domestic and foreign companies. In fact, the moves may encourage other governments to tighten regulations against dominant US-based platforms and services that over the years have been accused of inciting ethnic violence, undermining election integrity, and working with US intelligence agencies. While few countries have done more than the United States over the decades to develop and promote the global uptake of a free and open internet, this year once again signaled the decline of US leadership in cyber diplomacy and a broader retreat by Washington from international cooperation to zero-sum thinking.

The United States has now experienced four consecutive years of decline in internet freedom.

Information Isolation: Censoring the COVID-19 Outbreak

Information can be the difference between life and death. The coronavirus pandemic has underscored how important internet access is to protecting one's own health, staying informed, and keeping in contact with family and friends. From the onset of COVID-19, however, political considerations clashed with concerns about public health and free expression. Authorities blocked legitimate websites, ordered the removal of unwanted content, and most egregiously, shut down internet service altogether. Officials have reinforced these controls by criminalizing more categories of online expression and arresting journalists, activists, and members of the public for speaking out about the government's performance.

Blocking websites and deleting unwanted information

To suppress unfavorable health statistics, critical reporting, and other COVID-19 content, governments in at least 28 of the 65 countries assessed by *Freedom on the Net* blocked websites or forced users, social media platforms, or online outlets to delete information. Nowhere has censorship been more sophisticated and systematic than in China, whose authorities rushed to control the global narrative on their initial unwillingness and inability to contain the outbreak in Wuhan. Moderators censored millions of pieces of content containing over 2,000 keywords related to the pandemic on the leading communication platform WeChat and the live-streaming platform YY, affecting both criticism of the Chinese Communist Party and innocuous questions or observations about the virus. Online news outlets were also given strict orders about how to report on the virus: no publishing unofficial sources, no engaging in "independent reporting," and certainly no "sensationalizing" coverage on a range of topics, including physician Li Wenliang, one of the first whistleblowers from Wuhan, whose death from the virus in early February triggered a rare nationwide outcry calling for freedom of speech.

Following Beijing's lead, the government in nearby Bangladesh blocked the BenarNews website and a mirror site of the Swedish-based investigative outlet Netra News after they reported on a leaked internal memo from the United Nations and the World Health Organization about the country's rising case numbers. The document warned of the collapse of the country's health system and predicted up to two million deaths. Bangladeshi authorities also turned to crude intimidation to silence reporting that contradicted the government. Military intelligence officials warned the mother of Netra News's editor in chief against "tarnishing" Bangladesh's image. Politicians affiliated with the ruling party assaulted four journalists after a Facebook Live event in which it was alleged that there were irregularities in the government's distribution of aid during lockdowns.

Egypt's Supreme Council for Media Regulation ordered service providers to block several news outlets in March and April, accusing them of spreading false information. The outlet Darb, owned by the opposition Socialist Popular Movement Party, was blocked after it questioned human rights and health conditions in Egyptian prisons and called for the release of people who were incarcerated. The blocks were part of a broader crackdown on the information space. Officials revoked the credentials of a *Guardian* journalist who reported on medical research that estimated a higher number of cases than was acknowledged by government statistics. Separately, after an editor of a local newspaper challenged official COVID-19 data in a Facebook post, he was detained at a police station for a month before criminal charges were brought.

In Venezuela, a country already ravaged by an economic, political, and human rights crisis before the pandemic struck, de facto president Nicolás Maduro has coupled censorship with a series of false assertions, including claims that the virus is a "bioterrorist" weapon and that it can be prevented or treated with homemade lemongrass tea. Meanwhile, authorities blocked a website with information about the virus that was created by the opposition-controlled National Assembly and Juan Guaidó, who has struggled to gain recognition as the country's acting president. Police and other officials loyal to Maduro have also temporarily detained journalists and forced them to delete online content about the virus' spread or conditions in hospitals.

WHERE COVID-19 INFORMATION IS (AND ISN'T) CENSORED

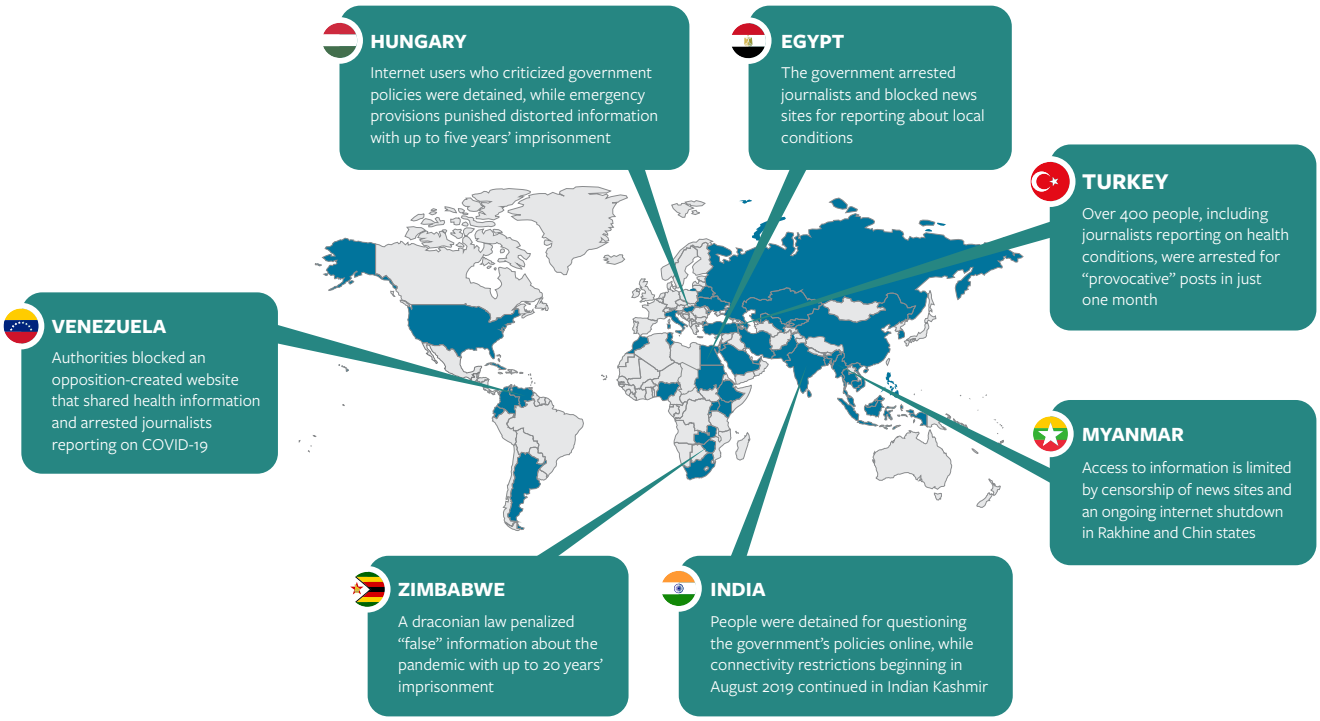
Governments are using the pandemic as a pretext to crack down on free expression and access to information.

28 countries
Websites or **social media posts censored**

13 countries
Government-imposed **internet shutdowns** during the pandemic

20 countries
New or expanded **laws restricting online speech**

45 countries
Internet users **arrested or detained** for COVID-19-related speech



President Alyaksandr Lukashenka of Belarus broadly dismissed the pandemic, referring to it as a "psychosis" and recommending vodka and other folk remedies to maintain health. The government largely sought to shout down contradictory information, though it periodically resorted to outright censorship. A web portal in the city of Bobruisk, for example, was forced to delete an interview in which a nurse discussed working conditions and problems with testing, while a regional state website removed COVID-19 statistics that contradicted those released by the Ministry of Health. Anger over Lukashenka's rigged August reelection bid, combined with frustration about the government's failure to take the pandemic seriously, galvanized mass protests in the country. The regime responded with even more repression, including violence against protestors, arbitrary detentions and torture, and several disruptions to internet connectivity.

Keeping populations in the dark

Governments have imposed internet shutdowns in at least 13 countries since January 2020, limiting people's ability to obtain timely information about the pandemic or use digital tools to access health care, education, and other necessary services. Long-term connectivity restrictions left some populations largely unaware of the virus as it spread rapidly around the globe in the first months of the outbreak. These shutdowns are notably concentrated in the home territories of historically marginalized groups. Access to the internet is an internationally recognized human right, and this year's network disruptions constitute an especially cruel form of collective punishment against specific ethnic and religious populations.

The government of Ethiopia restricted internet and phone services in parts of the Oromia Region from January to April 2020, as the military clashed with an Oromo rebel group. The

shutdown sharply restricted access to information about the pandemic for millions of Ethiopians in a region with poor health infrastructure, and where the country's first person confirmed to have the virus was reported to have traveled in March.

In Myanmar, which alongside Kyrgyzstan suffered this year's largest score decline, mobile internet service has been cut off since June 2019 for over a million people living in villages in Rakhine and Chin States—areas where the military has committed atrocities against the Rohingya and other groups. Officials in March also blocked regional and ethnic news sites, further marginalizing and endangering populations that have long been on the receiving end of the regime's egregious human rights abuses. The service and access disruptions severely limited residents' ability to initially learn of the virus's existence and then to obtain information about its spread. Across the border in Bangladesh, the internet was shut off for 11 months in the densely populated Cox's Bazar refugee camp starting in September 2019. The camp's nearly one million Rohingya residents, who sought safety there from genocidal violence in Myanmar, are consequently unable to access basic news, including lifesaving information about the pandemic.

High-speed internet service has been similarly suspended in parts of Jammu and Kashmir since August 2019, when India's central government embarked on a crackdown to enforce its revocation of the state's autonomy. Such restrictions have been disastrous for health care in the region. Doctors warned that the shutdown had isolated them from foreign colleagues and information about best practices in treating COVID-19. However, government abuses extended far beyond Kashmir, with health professionals across India facing intimidation and detention for speaking out online about unsafe working conditions.

Long-term shutdowns in Pakistan's border regions, including one that has lasted more than three years in the former Federally Administered Tribal Areas, also continued during the pandemic. A student petitioned the Islamabad High Court to restore mobile service, citing the shutdown's impact on online education. While the court sided with the petitioner, service was apparently not restored.

Banning criticism and arresting those who speak out

The pandemic has exacerbated a global clampdown on free expression. In at least 45 of the 65 countries covered by *Freedom on the Net*, activists, journalists, or ordinary members of the public were arrested or criminally charged for online speech related to COVID-19. Authorities justified the arrests through a myriad of laws that criminalize expression deemed to cause panic, instigate violence, spread hate, or insult officials, among other perceived harms. In at least 20 countries, governments cited the pandemic emergency to impose additional vague or overly broad speech restrictions. The measures most often criminalized the spread of "false" information or content that could damage "public order." By passing new laws and arresting individuals for nonviolent speech, leaders attempted to control narratives about the virus's spread, the government's performance, and the negative social and economic implications of lockdowns.

> Network disruptions constitute an especially cruel form of collective punishment against specific ethnic and religious populations.

In one of the world's harshest examples, Zimbabwe's emergency provisions have put internet users at risk of up to 20 years in prison for spreading false information about the pandemic. At least three people now face the draconian penalty after sharing allegedly false information about lockdowns on WhatsApp. In another arrest under a separate law, an investigative journalist in the country was charged and held in pretrial detention for six weeks after reporting on Facebook that the president's son was involved in corruption tied to health-related procurement contracts.

A government crackdown on free expression and "fake news" in Thailand has ramped up amid the pandemic. Implemented in February 2020, an emergency decree outlaws online speech that could threaten security, may instill fear, or is intentionally distorted to cause misunderstanding. Individuals accused of such offenses can be charged under the country's repressive Computer Crime Act, which has long been used to punish activists and journalists for their work, or under the emergency decree itself. In March 2020, an artist was arrested after stating on Facebook that he did not go through a screening process for the virus at an airport. A whistleblower also faces charges after posting on Facebook about shortages of medical supplies and related corruption.

The Philippines' emergency law has served as another tool for President Rodrigo Duterte to consolidate his power and intimidate critics. A last-minute addition to the law punishes the spread of "false information" with up to two months in prison and a fine of 1 million pesos ($19,600). Dozens of people have since been investigated, arrested, and charged, including two online journalists who simply shared a local mayor's social media posts about the virus. Prime Minister Hun Sen of Cambodia has similarly repurposed the health crisis to continue arresting and charging members of the banned Cambodian National Rescue Party for their social media posts. Sovann Rithy, founder of an online news outlet, was separately charged for quoting a speech by the prime minister himself.

Azerbaijan's parliament expanded the legal definition of "prohibited information" in an effort to suppress more online speech in what was already a restrictive environment. The amended Law on Information, Informatization, and Information Protection now encompasses "false" information that threatens life or health, causes property damage, disrupts transport, or has "other socially dangerous consequences." One journalist was arrested and sentenced to 25 days in detention after police demanded that he remove social media posts on the social and economic impact of the pandemic.

Rather than passing new emergency measures to criminalize speech, Turkey's President Recep Tayyip Erdoğan used his existing legal toolbox to reprimand individuals who challenged the government's tightly orchestrated propaganda campaign. Over 400 people, including journalists and doctors, were detained in March alone for their "provocative" and "abusive" social media posts about the pandemic. After a city medical association posted on Twitter about the deaths of health workers and a lack of personal protective equipment, two doctors involved with the association were detained, interrogated, and barred from traveling abroad.

Authorities with a track record of quashing dissent are not alone in imposing such restrictions. Even governments that have historically protected online free expression have responded disproportionately to pandemic-related speech. South Africa rolled out state-of-disaster regulations that bar statements through "any medium, including social media" if they are intended to deceive someone about the virus, government actions, or a person's infection status. Celebrity entertainer Somizi Mhlongo was criminally charged after suggesting on Instagram that the country's transport minister planned to extend the country's lockdown.

In Hungary, where internet freedom had not yet been heavily affected by a precipitous decline in democracy over the past decade, the government introduced provisions as part of its "state of danger" legislation that prescribed a five-year prison term for publishing false or distorted information on the pandemic. One opposition-affiliated activist was taken into custody and accused of "obstructing efforts to combat the pandemic" by posting about a government policy to clear hospital beds for COVID-19 patients. Another man was accused of fearmongering and detained after he called Prime Minister Viktor Orbán a "cruel tyrant" on Facebook while discussing lockdown measures. Health workers and other professionals involved in the fight against COVID-19 have reported that they are less likely to speak publicly and openly for fear of retaliation.

> Users in at least 45 out of 65 countries were arrested or criminally charged for online speech related to COVID-19.

Dealing with dangerous speech

In what has been described as an "infodemic," inaccurate and unscientific posts have contributed to the loss of life from COVID-19, either due to their flagrant disregard for the danger posed by the virus or because they promote dangerous or ineffective treatments. President Jair Bolsonaro in Brazil and President Donald Trump in the United States have both suggested at times that the pandemic is no more dangerous than common influenza, and they have recklessly promoted unsafe or untested treatments. Such efforts are consistent with their administrations' history of rejecting science in making public policy. Individuals from countries as varied as Nigeria, Vietnam, and Iran have died or been hospitalized after poisoning themselves with alcohol, bleach, hydroxychloroquine, and other substances that some have touted as miracle cures.

State and nonstate actors are using the pandemic to promote conspiracy theories and pseudoscience that aligns with their nationalist and xenophobic political goals. High-ranking members of India's ruling Hindu nationalist Bharatiya Janata Party made Islamophobic statements after the government linked a March meeting

of a Muslim missionary group to a spike in coronavirus cases. The statements echoed anti-Muslim online news stories and Twitter hashtags like #CoronaJihad and #MuslimMeaningTerrorist that falsely accused Muslims of deliberately spreading the virus. Numerous Muslims have been beaten in the country, and at least one boy lost his life, as a result of similar false rumors. After Cambodia's Ministry of Health published a Facebook post identifying adherents of "Khmer Islam" as one of the groups that had contracted the virus, social media trolls launched a barrage of hateful comments at the country's small Muslim community. In Sri Lanka, the government has restricted the religious freedom of Muslims by mandating the cremation of all those killed by COVID-19, despite evidence that burial does not spread the virus. As long as pandemic-related disinformation is being exploited for a government's political gain, it is likely to proliferate online, to the detriment of public health and safety.

Ensuring that the information environment remains open, safe, and free

Governments have a duty to foster a reliable and diverse information space, especially during major events—such as elections, protests, and pandemics—that can serve as catalysts for the spread of false and misleading content. The amplification of rumors and falsehoods by public officials and privately run platforms gives such material a shroud of legitimacy. At the same time, arresting those responsible or deleting their content can fuel conspiratorial claims that powerful interests have something to hide. States should only prevent access to information in limited cases, when the action can be defended as both necessary to serve a legitimate purpose and proportionate to the threat.

Similarly, tech platforms should protect free expression and access to information whenever possible, adopting a minimalist approach to interventions as outlined by international human rights standards. Content moderation practices must be robustly transparent, apply consistently across issues and ideologies, include independent avenues of appeal and genuine opportunities for redress, and feature human oversight of any automated systems. Tech companies should also use their immense power over the information space to push out verifiable information from public health authorities.

Digital news media that are independent, diverse, and free are also essential to promoting a democratic information space. The media can conduct digital literacy campaigns, investigate propaganda offensives and their origins, and hold officials accountable for violating human rights. Journalists contributing to online outlets should be given full access to state officials and resources, a safe environment in which to work, and protection from online harassment and intimidation.

Restrictions to the digital environment can have far-reaching social, political, economic, and personal consequences. During the pandemic, digital tools have been essential for staying connected with loved ones, engaging with health care providers, and worshipping freely. As people continue to work remotely and more students come to rely on online learning, gaps in access will be a drag on the economy and exacerbate existing inequities in education and employment, especially when connectivity restrictions target regions where marginalized ethnic groups reside. A lack of internet access also affects people's ability to participate politically. Ahead of elections in the United States and around the world, for example, online resources play an important role in facilitating voter registration, requests for mail-in ballots, and public education about the candidates and issues at stake. Protecting access to the free and open internet is fundamental for the future of democracy.

METHODOLOGY AND DATA SOURCES

Freedom on the Net identified and tracked five indicators relating to COVID-19 and censorship—internet shutdowns, website blocking, content removal, emergency laws and policies, and arrests of internet users—in 65 countries around the world. Freedom House's analysts conducted thorough research of news websites, blogs, social media content, academic journals, and law and policy documents, often across multiple languages. Throughout the process, the analysts worked in close partnership with the activists, journalists, and lawyers who research and write the *Freedom on the Net* country reports. Our team also drew on the excellent work of other nongovernmental organizations, including resources related to COVID-19 that are maintained by the Committee to Protect Journalists, the International Center for Not-for-Profit Law, and the International Press Institute. Visit freedomonthenet.org to access and download other country-specific data and sources used in this essay.

False Panacea: Abusive Surveillance in the Name of Public Health

Brick by brick, governments and companies responding to the public health crisis are laying a foundation for tomorrow's surveillance state. Opaque smartphone apps collect biometric and geolocation data in an effort to automate contact tracing, enforce quarantines, and determine individuals' health status. State agencies are gaining access to larger swaths of user data from service providers in a process that lacks oversight and safeguards against abuse. Police and private companies are accelerating the rollout of advanced technologies to monitor citizens in public, including facial recognition, thermal scanning, and predictive tools.

These systems have been deployed with little scrutiny or resistance. Most countries have yet to enact meaningful constraints on the collection and sharing of individuals' biological information, known as biometric data, by state and corporate actors. Meanwhile, the past two decades of rapid technological change have already implanted surveillance into nearly every aspect of governance and commercial activity, creating an alarming amount of information that can be vacuumed up and manipulated by state and nonstate actors alike.

History has shown that new state powers acquired during an emergency tend to outlive the original threat. In their responses to the 9/11 terrorist attacks, governments around the world accelerated the militarization of law enforcement, gave state agencies broader mandates with less oversight, enhanced suspicion of and discrimination against marginalized populations, and normalized mass surveillance. The COVID-19 pandemic could serve as the catalyst for similar harms. Alarmingly, authorities in many countries have exploited the public health crisis to institute new and intrusive forms of surveillance, gaining novel powers of social control with few checks and balances.

> Authorities have exploited the crisis to institute intrusive forms of surveillance with few checks.

The need for checks on runaway data collection

Contact tracing is vital to managing a pandemic. However, digital monitoring programs, which can sweep up more identifiable information than manual testing and tracing, are being implemented hastily, often outside of the rule of law and other structures of oversight and accountability that can ensure the protection of basic rights. Data collected from smartphone apps or by state agencies—such as one's location, names, and contact lists—can be paired with existing public and corporate datasets to reveal intimate details of people's private lives, including their political leanings, sexual orientation, gender identity, religious beliefs, and whether they receive specialized forms of health care. The conclusions drawn about an individual from these data can have serious repercussions, particularly in countries where one's opinions or identities can lead to closer scrutiny and outright punishment.

The pandemic is ushering in a new age of digital social sorting, in which people are identified and assigned to certain categories based on their perceived health status or risk of catching the virus. Once flagged, a given group may be subjected to stigmatization and marginalization. They can face limits on their ability to access public services or education, return to work, send their children to day care, visit a shopping mall, or use public transport. Such programs may even take into consideration the actions of family members, housemates, or neighbors, penalizing individuals by association.

These public health surveillance systems will be remarkably difficult, if not impossible, to decommission. As with national security matters, state agencies will always argue that they need more data to protect the country. There will also be great demand for health-related information from marketers, insurers, credit agencies, and any other industries that could profit from it. Given that the US National Security Agency itself has suffered high-level breaches affecting some of its most sensitive information, it is doubtful that such private actors will be able to defend the data from cybercriminals and state-sponsored hackers.

SOME APPS TRACE COVID-19, OTHERS TRACK YOU

Greater public deliberation and independent oversight are needed to blunt the expansion and entrenchment of mass surveillance practices. At the very least, authorities must prove that a proposed measure is necessary and fit to purpose. Many new programs, for example, incorporate mobile-device location data to assist contact tracing, but the technology may not be precise enough to discern whether two people were at a safe distance from each other, and systems based on satellite signals are ineffective if the individuals are indoors. Such uncertainty is especially problematic if the location records are used to penalize people for not complying with quarantine or social-distancing rules.

Even if public health experts can demonstrate a monitoring program's necessity and effectiveness, it must include independent oversight, transparency, and narrowly tailored rules that minimize what data are collected, who collects them, and how they can be used. Without such robust safeguards, the marginal benefits of pandemic surveillance are outweighed by the threat they pose to democratic values and human rights.

A proliferation of surveillance apps

Smartphone apps have been deployed for contact tracing or ensuring quarantine compliance in at least 54 of the 65 countries covered by this report. While these apps may make it easier for individuals to identify whom they have interacted with over a certain period of time, their rapid and nearly ubiquitous rollout presents an immense risk to privacy, personal security, and broader human rights. Developers have largely ignored established principles for privacy-by-design, an approach meant to ensure that privacy considerations are built into a tool's architecture and software. Most apps are closed source, which does not allow for third-party reviews or security audits, and in practice there are few opportunities to appeal and redress any abuses. Moreover, in many countries, cybersecurity standards may have been made intentionally weak in order to facilitate broader data collection by state authorities.

These smartphone programs automatically gather sensitive information on where users live, with whom they reside, their daily routines, their casual interactions, and much more. Many of the apps ask for demographic and other data to facilitate

The rapid and nearly ubiquitous rollout of pandemic-related apps presents an immense risk of privacy, personal security, and broader human rights.

user identification, then send the files, unencrypted, to a centralized server located in government offices. Researchers have demonstrated how easily these data can be leaked to cybercriminals, security agencies, and even other apps running on individuals' phones. Some programs connect to additional surveillance technologies like facial recognition and electronic wristbands in order to verify users' identities and more closely monitor their movements.

India is home to several pandemic apps that pose human rights risks. Aarogya Setu, a closed-source app that has been downloaded by over 50 million Indians, combines Bluetooth and Global Positioning System (GPS) tracking to determine users' potential exposure and generates a color-coded "health status" to rate their risk of infection. Information collected from the government-backed app is stored in a centralized database, where it is shared with health institutes and other government agencies. More than a million people have been required to use it, and in at least one city, failure to download the app may result in criminal charges. Another closed-source app that collects and stores personal information, including GPS data, is Quarantine Watch, developed in partnership with the state government of Karnataka. The app requires users to send pictures of themselves accompanied by metadata on their geolocation to prove that they are complying with mandatory isolation. State officials have joked that "a selfie an hour will keep the police away."

Although India is currently considering a data-protection bill, standards for cybersecurity remain lax, and sensitive COVID-19 databases created by the new apps have already been breached. Millions of personal records from a symptom-checker app developed by Jio, a leading telecommunications provider, were shown to be accessible without a password on an online database. Even before the pandemic, the security flaws of the country's Aadhar biometric identification system led to numerous scandals involving data breaches. India is currently instituting a nationwide facial-recognition program that privacy advocates say could facilitate repression and discrimination. Separately, in October 2019 and June 2020, two reports revealed that government-linked spyware had been deployed against journalists and activists who drew attention to human rights violations in the country.

Mobile apps in Russia have added to the regime's growing surveillance apparatus. The Social Monitoring app accesses GPS data, call records, and other information and requests random selfies from users to enforce quarantine orders and other restrictions on movement. In just over a month, authorities imposed nearly 54,000 fines totaling over $3 million on users. The penalties were sometimes erroneous and arbitrary, with those tagged for fines including the wrong identical twin, a bedridden professor, and sleeping users who received selfie requests in the middle of the night. Moscow residents over the age of 14 must log onto a government website to state their planned movements; users receive a QR code that is then scanned by security personnel in order to verify that they have permission to be in a given location.

The Bahraini government's BeAware app is required for those in self-isolation or quarantine due to potential local exposure or a recent return from abroad. Individuals face fines of up to 10,000 Bahraini dinars ($26,000), a minimum three-month jail term, or both for failing to wear an electronic wristband or comply with the app. The program sends location and diagnostic information to a central government server and alerts authorities if an individual has strayed more than 15 meters from the phone. The government has a long record of monitoring dissidents for political reasons, including through the use of sophisticated spyware targeting the persecuted Shiite Muslim majority.

Saudi Arabia's Tetamman app also comes with a mandatory Bluetooth bracelet. Failure to comply with strict quarantine measures can result in up to two years in prison, a fine of 200,000 riyals ($53,000), or both. A security researcher has reported that the Saudi government may also be testing the contact-tracing tool Fleming, which was created by the Israeli company NSO Group. The government has already used NSO Group's other products to monitor and intimidate its critics. Authorities are strongly suspected of deploying the company's Pegasus spyware to access the communications of activists and journalists, including the journalist Jamal Khashoggi, who was ultimately killed by Saudi agents in 2018.

In Turkey, a new system called Hayat Eve Sığar (HES) combines contact tracing with a health status code. A positive HES code is compulsory for all domestic travel. While the Turkish government app is the most efficient way to secure

A visitor's temperature is taken with a thermal scanning device at the entrance to Edge Observation Deck at Hudson Yards on September 4, 2020 in New York City. Photo credit: Cindy Ord/Getty Images.

such a code, users can also text certain personal details to a phone number. The app emits Bluetooth signals to surrounding devices in order to facilitate contact tracing. It is used to monitor compliance with quarantine orders and sends data directly to law enforcement in case of violations. Government surveillance and the misuse of user data have been widespread in Turkey for years, and civil society has sounded the alarm about potential abuse of the new app.

Like the virus itself, quarantine and contact-tracing apps have had a disproportionate impact on certain populations. Singapore's migrant workers, who often suffer from poor housing and employment conditions, are specifically required to use apps for contact tracing, the recording of symptoms, and reporting of their health status, setting them apart from other residents. In Ukraine, dozens of individuals were left stranded in an active conflict zone: people without smartphones and internet access, mainly the elderly, were unable to download the government's mandatory Diy Vdoma self-isolation app and thus were not allowed to cross from separatist-controlled to government-controlled territory.

Private companies are also rapidly developing and selling health-code apps, which increasingly serve as gatekeepers for access to essential public services and the exercise of fundamental rights. COVI-Pass—a system designed by a British company—grants users a "VCode" to be scanned when entering office buildings, attending a sporting event, or walking in public. Individuals obtain color-coded results depending on their previous tests for the virus or its antibodies. COVI-Pass has already been sold to governments and companies in over 15 countries. Private companies in the United States have also expressed interest in requiring customers to use such coding systems, including airlines and hotels.

Amid the proliferation of problematic apps, some developers have attempted to create new products centered on privacy. An international consortium has supported the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) protocol. The Swiss team behind this project has opened up its source code for expert review in order to maximize cybersecurity and data privacy. In addition, tech giants Apple and Google jointly developed the Exposure Notification System application program interface (API). The opt-in software transmits random identification numbers via Bluetooth to surrounding smartphones and stores the numbers directly on the phone, rather than on centralized company or government servers. Users are notified if they interact with a person who has or is later identified as having tested positive for COVID-19.

The Google and Apple API allows health agencies to build their own apps using the firms' privacy-respecting architecture. Authorities in Estonia, Brazil, and the United States are rolling out apps using either DP-3T, the Exposure Notification System, or both. Estonians can also rely on the country's strong legal protections for privacy and transparency. However, Brazil's recent track record on privacy and surveillance raises concerns for digital contact tracing. For instance, in October 2019, President Bolsonaro signed a decree, without public consultation or debate, compelling federal agencies to share a range of citizen data, including health records and biometric information. The United States also lacks federal privacy laws that could limit the ways in which data stored on phones and by apps are accessed, sold, or used.

Decentralized, opt-in, and Bluetooth-based contact-tracing tools are a promising alternative to more invasive, mandatory apps that feature centralized control. However, even they are not free of privacy and other risks. Smartphone apps in general are opaque about how they collect, store, and process data, and how and with whom they share information. Other apps on a user's device, for example, may gain access to sensitive data stored there by the contact-tracing program, allowing them to sell the material to advertisers, insurers, credit agencies, or other data brokers. Proximity tracking is also vulnerable to being spoofed or hacked. Most importantly, no contact-tracing app will be useful or effective unless it is widely adopted and deployed in an environment with robust testing, manual contact-tracing systems, and a well-resourced public health infrastructure.

Tapping into telecommunications data

In at least 30 countries, governments are using the pandemic to engage in mass surveillance in direct partnership with telecommunications providers and other companies. New data-sharing initiatives may help authorities to conduct contact tracing and big-data analysis to understand the virus' spread. However, the expanded data collection in many countries lacks transparency, proportionality, and privacy protections, posing clear risks to fundamental freedoms. It is particularly worrisome that national security and military agencies have been tasked with this work in some cases.

In Pakistan, the government has retooled an antiterrorism system to support "track and trace" efforts. The secretive program was developed by the Inter-Services Intelligence (ISI) agency, which has been implicated in enforced disappearances and other flagrant human rights abuses. It allows for "geofencing" to identify all of the people who have passed through a specific area at a specific time. There are separate reports of intelligence agents tapping the phones of hospital patients to determine whether their friends and family express having symptoms themselves. Officials also have access to a national biometric database containing information on over 200 million citizens. Little is publicly known about the overall program, though reports indicate that data can be passed on to police, health departments, and provincial government agencies. Patients who have tested positive, including health workers, have had their personal information leaked online, with severe consequences for their social standing and emotional well-being.

Sri Lanka has also integrated its defense apparatus into its pandemic response. Military intelligence officials are obtaining personal data from mobile service providers to identify people who have interacted with confirmed patients or evaded quarantines. Sri Lanka's military has been accused of gross human rights violations and extrajudicial killings in the past, and since the 2019 presidential election, the authorities have escalated their intimidation and harassment of journalists, human rights defenders, and others they perceive as critics.

South Korea has been comparatively effective at containing its coronavirus outbreak, but its Infectious Disease Control and Prevention Act (IDCPA) permits broad surveillance, raising questions about epidemiological necessity and proportionality. Officials have pulled information from credit card records, phone location tracking, and security

cameras—all without court orders—and combined it with personal interviews for rapid contact tracing and monitoring of actual and potential infections. Credit card histories reveal intimate details about people's lives that go far beyond what is needed for contact tracing; people's purchases can indicate their sexual orientation and religious beliefs, for example. South Korean officials have at times publicized patients' gender, age range, and movements, which has fueled online ridicule, scrutiny, and social stigma. On the positive side, IDCPA does include important sunset provisions, requiring pandemic-related data to "be destroyed without delay when the relevant tasks have been completed."

The government in Ecuador has taken a multifaceted approach to surveillance amid the pandemic. The country's ECU 911, a public security network built mainly by Chinese firms with close ties to the regime in Beijing, has been actively collecting input from thousands of surveillance cameras, geolocation data, and police records to engage in "smart" analysis. ECU 911 is being incorporated into a new public health platform, which aggregates location data from satellite and mobile phones as well as information from the country's COVID-19 app, including names, national identification numbers, birth dates, and geolocation records. National and local authorities are provided information from the platform's database for contact-tracing purposes, to ensure quarantine compliance, and to identify any large gatherings at places such as schools, homes, and funeral sites. There is little transparency as to how long data are stored, by whom they could be used, and for what purposes.

In April 2020, state governors in Nigeria announced a new partnership with MTN, the country's leading telecommunications provider, to model how vulnerable their states are to the pandemic based on subscriber information. Only two months earlier, the government and security forces were found to have been accessing mobile data records to identify and arrest journalists. Armenia's parliament voted in March 2020 to grant surveillance agencies the ability to obtain telecommunications metadata from service providers, including phone numbers and the location, time, and other metadata of calls and messages, without judicial review. The data were meant to be used to identify individuals who may have encountered the virus and to monitor those in isolation, but the lack of transparency and oversight made it unclear how the records would or could be used in practice.

Some governments have taken preliminary steps to reduce privacy risks to users and are instead accessing aggregated and anonymized datasets to guide public health policy. In Australia, for example, the telecom company Vodafone provided the government with the location data of millions of people in an aggregated and anonymous format, allowing it to understand population movements and determine broad compliance with social-distancing restrictions.

> In at least 30 countries, governments are using the pandemic to engage in mass surveillance in direct partnership with telecommunications providers and other companies.

In the United States, the mobile advertising industry handed over aggregated and anonymized location data to federal, state, and local governments. Authorities aimed to centralize the location data on people in over 500 cities in order to analyze how the disease was spreading. By requesting data from the advertising companies rather than mobile service providers, however, government agencies bypassed the minimal privacy-oversight mechanisms built into US law. The White House and the Centers for Disease Control and Prevention (CDC) have also reportedly negotiated with tech platforms about accessing aggregated and anonymized location data.

While anonymized data can be less invasive than individualized information, the records can be rendered identifiable, or deanonymized, when combined with other datasets or analyzed by big-data tools that are designed to find patterns in content from disparate sources. This potential means that anonymized and aggregated information remains vulnerable to exploitation or misuse by both governments and nonstate actors. The risk is compounded by the disproportionate surveillance laws and the lack of robust privacy protections in many countries, including both Australia and the United States.

Limited access to certain forms of data may be helpful for tracking how the virus spreads and to inform current and future responses to health crises. However, any sharing of digital information must be transparent, subject to independent oversight, and governed by the human rights principles of necessity and proportionality. The information

collected should be firewalled from other uses and generally destroyed after the virus is brought under control. This will help ensure that authorities and private companies cannot easily repurpose health data to serve political, law enforcement, or commercial goals.

Rolling out the AI surveillance state

No country has taken a more comprehensive and draconian approach to COVID-19 surveillance than China, where the pandemic began. Over the past two decades, the Chinese Communist Party has built the world's most sophisticated and intrusive surveillance state, consisting of both low- and high-tech elements. More recently, as China seeks to become a global leader in AI technology by 2030, authorities have experimented with machine learning, big data, and algorithmic decision-making in service of the regime's politically repressive "social management" policies. Automated systems flag suspicious behaviors on the internet and, increasingly, on public streets using the world's largest security-camera network. Since January, authorities have combined their existing monitoring apparatus and biometric records with invasive new apps and new opportunities for data collection.

After the coronavirus struck, regional officials partnered with major Chinese tech firms Alibaba and Tencent to develop "health code" apps. The prevailing software assigns individuals a QR code and low (green), medium (amber), or high (red) risk ratings depending on factors such as their location history and self-reported symptoms, although neither authorities nor the companies provide further information on how the risk levels are calculated. A green code has been required to access certain public spaces and office buildings. Although there are variations among the dozens of apps used in each province or municipality, an analysis by the law firm Norton Rose Fulbright found that the privacy policy of Beijing's app does not incorporate strong privacy-by-design principles or state any time limit on the retention of data. A *New York Times* investigation showed that the Alipay Health Code app automatically shared data with the police.

No country has taken a more comprehensive and draconian approach to COVID-19 surveillance than China.

As the initial outbreak was brought under control in China, certain health code apps were rolled back in cities like Shanghai. Conversely, in May, health officials in Hangzhou proposed to expand the city's app system from simple color codes into personal "health scores" that would reflect people's sleep patterns, alcohol consumption, smoking habits, and exercise levels. The proposal led to uproar among users and even earned a rare rebuke from state-run media. The concept has some similarities to experiments with government "social credit" systems and pilot apps run by corporations such as Ant Financial's Sesame Credit, which track users' personal and online behavior. Appearing on a blacklist maintained by municipal or provincial authorities can result in restrictions on movement, education, and financial transactions. By contrast, highly rated Sesame Credit users can win privileged access to private services, deposit waivers, and shorter lines at airport security. As of now, the government and privately run systems are maintained separately, although there are some indications they may be merged in the future.

Chinese authorities have also compelled state-owned telecoms and private tech companies to share data with public security bodies. Data terminals have been installed at train stations, hotels, and other high-traffic locations in order to rapidly collect information on individuals' movements and location. Hundreds of individuals have issued complaints regarding COVID-19-related data leaks and privacy violations, with some observers calling for greater personal data protections to rein in the chaotic data-sharing prompted by the health crisis. Such demands add to rising pressure from Chinese netizens since 2018 in favor of data-protection legislation that would limit the ability of governments and corporations to access and use personal information.

Authorities are also testing the patience of residents through increasingly intrusive video and facial-recognition surveillance. Individuals have complained of being asked to install webcams inside their homes and outside their front doors. Facial-recognition companies like Hanwang claim that they can now identify people even if they are wearing a mask. The search engine giant Baidu announced in February that it had created face-scanning software to help the government identify people who are not complying with mask-wearing requirements. In March, authorities upgraded facial-recognition cameras in 10 cities with thermal detection technology, which can supposedly scan crowds of people and identify who has a fever.

MAPPING CHINA'S SURVEILLANCE STATE

The Chinese government has taken the most comprehensive and draconian approach to COVID-19 surveillance.

Although China's surveillance systems remain the most advanced and pervasive in the world, governments in countries across the democratic spectrum are rolling out biometric and AI-assisted surveillance with few or no protections for human rights. A network of over 100,000 cameras with facial-recognition capabilities in Moscow was reportedly used to enforce quarantines in March. Paris's mass transit system has begun testing AI video cameras created by tech company Datakalab to compile statistics on riders wearing masks. Meanwhile, companies based in the United States and Europe are pitching tools to governments, schools, restaurants, and other institutions, claiming to be able to identify people with fevers at a distance. A biometric border-control system sold by the German company DERMALOG is being piloted in Bangkok, aiming to match facial recognition with fever detection to identify travelers who may have communicable diseases.

Many of the high-tech tools unveiled over the past year are not effectively tackling the crisis at hand. Instead they reinforce existing political repression and social inequity because of their dependence on inaccurate or biased data and the realities of racism and discrimination that shape the contexts in which they are used. Facial recognition, for example, is particularly unreliable for people of color and people who are transgender. One study found a 99 percent accuracy rate for white men, while the error rate for women who have darker skin reached up to 35 percent. Another study identified Native Americans as having the highest false-positive rates of any ethnicity in the United States.

> Governments across the democratic spectrum are rolling out biometric and AI-assisted surveillance with few or no protections for human rights.

Other forms of biometric technology, including those that employ forced DNA collection and emotion recognition, are similarly affected by discriminatory inaccuracies and can be just as easy to abuse. Biometric systems can collate information from face scans, iris scans, fingerprints, and DNA, and then use opaque algorithms to identify, track, and categorize people. Among other potential applications, such technology could be used to identify and monitor individual protesters, members of ethnic and religious minority groups, independent journalists, or any other group that is deemed a threat to those in power.

If such technologies are allowed to be introduced, it is imperative that they be governed by robust laws and regulations to protect fundamental rights and prevent the normalization of harmful and intrusive monitoring. The dangers they pose to freedom and democracy are simply too grave to ignore.

Living in the black box

The urgent need to combat COVID-19 has only accelerated the expansion of biometric surveillance and algorithmic decision-making in fields including health care, policing, education, finance, immigration, and commerce. The public should be deeply skeptical of this trend, in which private companies and government authorities promise purely technological solutions to problems that in fact require concrete economic, societal, or political action to address.

> Only collective action on a global scale can halt the momentum of the emerging AI surveillance state.

Opaque algorithms are quickly replacing human judgment in vital areas of human life, and the results are likely to create new inequalities and further disadvantage those who were already vulnerable to discrimination. In the context of health care, for example, predictive technology could be used to determine whether certain people or groups are more likely to contract or spread a virus, then bar them from public spaces. Similarly, in the criminal justice system, people deemed suspicious based on an automated analysis of inaccurate or discriminatory data could be flagged for enhanced monitoring or even arrest.

As commercial enterprises, security agencies, and government bureaucracies come to trust and rely on digital technology, with all its flaws, there is a risk that the technology itself could effectively become the authority, rather than a tool used to implement human decisions. Policies determined by an inscrutable automated system cannot be examined or corrected using traditional democratic procedures. Humanity currently maintains some understanding of why an algorithm generates one output rather than another, but AI could ultimately remove what is known as "explainability"—and with it any sense of transparency, supervision, or accountability for injustice.

The future of privacy and other fundamental rights depends on what we do next. As schools reopen, people head back to offices, and travel resumes despite the ongoing pandemic, the push for mandatory mobile apps, biometric technology, and health passports will only grow. It is vital for the public to consider whether certain new forms of surveillance are necessary or desirable in a democratic society, to resist overblown or unrealistic promises from promoters of high-tech tools, and to push elected officials to build strong privacy protections and other democratic safeguards into law. Individual countries can take the lead, but only collective action on a global scale can roll back current excesses and halt the momentum of the emerging AI surveillance state.

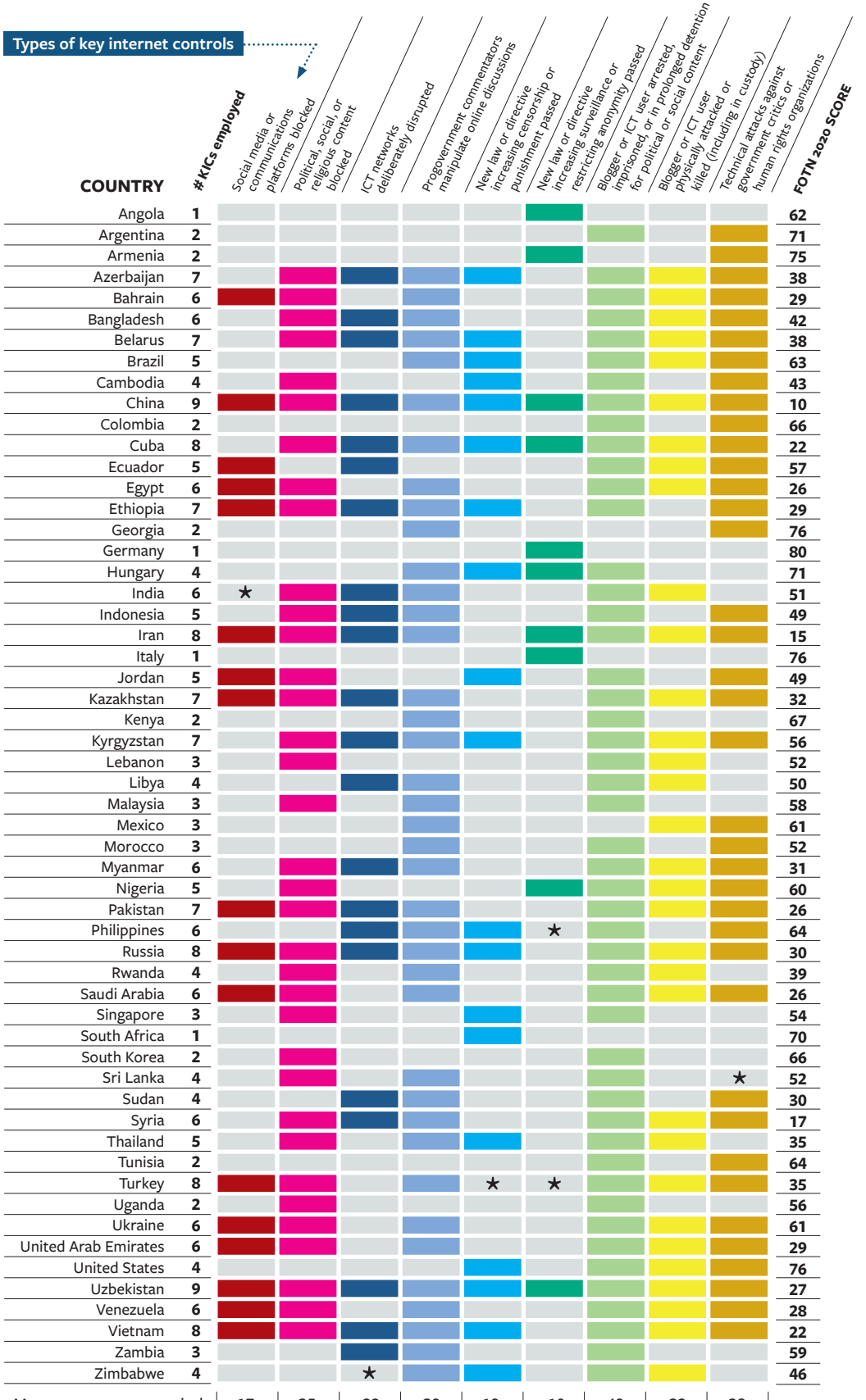
METHODOLOGY AND DATA SOURCES

Freedom House identified a series of COVID-19-related surveillance data points and collected the relevant information on all 65 countries covered by *Freedom on the Net*. The resulting database was partly informed by the individual *Freedom on the Net* country reports written by external analysts. Freedom House staff conducted additional research and drew on the work of various other organizations, including the MIT Technology Review's COVID Tracing Tracker, the COVID-19 Digital Rights Tracker from Top10VPN.com, the Centre for Internet Society's Digital Identities project, Privacy International's global COVID-19 response tracker, and OneZero's COVID surveillance analysis of 34 countries. Visit freedomonthenet.org to access and download other country-specific data and sources used in this essay.

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 2019 to May 2020; cells with an asterisk (*) represent events that occurred between June and September 2020, 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
Australia	76
Canada	87
Estonia	94
France	77
Iceland	95
Japan	75
Malawi	60
The Gambia	49
United Kingdom	78



FREEDOM ON THE NET 2020

Status	Countries
FREE	15
PARTLY FREE	28
NOT FREE	22
Total	**65**

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

Recommendations

FOSTERING A RELIABLE AND DIVERSE INFORMATION SPACE

For Policymakers

Reject undue restrictions on access to information and free expression, especially during a pandemic. Governments should support and maintain access to the internet and 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 such services through standard democratic mechanisms, including legislation passed in consultation with civil society experts and affected stakeholders, rather than resorting to national security orders and emergency measures.

Take action to address the digital divide. With jobs and schooling moving online as a result of COVID-19, the repercussions of unequal access to the internet are worsening. 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 to lend electronic devices to individuals who need them. Longer-term efforts could include expanding access and building internet infrastructure for underserved areas and populations, ensuring that connectivity is affordable regardless of income level, and enacting strong legal protections for user privacy and net neutrality.

For the Private Sector

Ensure fair and transparent content moderation. To accomplish this, private companies should do the following:

- Prioritize users' free expression and access to information, particularly for content that can be considered journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression.
- Clearly and concretely define in their 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, and design changes that grant users more control over their information digest.
- Ensure that content removal requests from governments are in compliance 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.
- 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 a meaningful opportunity for human review.

For Civil Society

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

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.

Build digital literacy among the public. Civil society organizations should educate netizens about how to spot disinformation and misinformation on social media, addressing topics such as altered content, so-called deepfake videos, suspicious spelling or phrasing, and inadequate citation. Organizations should also inform internet users about how to report false or suspicious content and how to flag this content for friends and family.

PROTECTING HUMAN RIGHTS FROM INTRUSIVE SURVEILLANCE

For Policymakers

Ensure that new surveillance programs meet international human rights standards for necessity, proportionality, and independent oversight. New surveillance programs meant to help combat COVID-19 must first be shown to be necessary—in the view of public health experts—for containing the spread of the virus. Any program should also be narrowly tailored, minimizing what information is collected, who collects it, and how it can be used. Any sharing of data must be transparent and subject to independent review. The information collected should be firewalled from other uses and generally destroyed after the virus is brought under control, so that authorities and private companies cannot access it later for political, law enforcement, or commercial purposes. Any programs involving the use of smartphone apps should be voluntary, with no participation requirements for access to public services.

Enact robust data privacy legislation and protect encryption. In the United States, policymakers should pass a federal electronic privacy law that provides robust data protections and harmonizes rules among the 50 states. They should also resist legislative attempts to undermine encrypted services, including through the use of "back doors." Individuals should have control over their information and the right to access it, delete it, and transfer it to the providers of their choosing. Governments should have the ability to access personal data only in limited circumstances as prescribed by law, subject to judicial authorization, and within a specific time frame. Companies should also be required to disclose in nontechnical language how they use customer data, details on third parties that have access to the data, and how third parties are allowed to use the data. Companies should also be required to notify customers in a timely fashion if their information is compromised. Given the technical measures—including cyberattacks—that both foreign and domestic actors use to access citizens' personal information, data privacy legislation should be paired with cybersecurity requirements concerning the collection and storage of user data.

Firmly restrict new surveillance technologies that employ biometrics and artificial intelligence. Lawmakers should pass a moratorium on the use of facial- and other affect-recognition technologies in sensitive areas such as law enforcement, education, employment, health care, and housing, and future legislation governing these technologies should be informed by additional research on their potential harms to human rights. State and local governments should follow the lead of municipalities in California, Oregon, Massachusetts, and other US states that have passed moratoria or bans on the use of biometric and AI surveillance.

Improve oversight of and create alternatives to algorithmic decision-making. Governments should be explicit about how, when, where, and why they use automated systems. Procurement processes for such technology should be transparent and include human rights–based impact assessments. Government agencies should create pathways to ensure human oversight and explanation, especially when algorithmic decision-making determines access to public services like education, health care, and housing. Automated systems should be routinely audited to ensure that they comply with antidiscrimination laws and other rights-based standards. Furthermore, governments should establish mechanisms for appeal and redress in cases of discrimination by algorithm.

For the Private Sector

Design public health apps with privacy and security in mind. Software developers should build privacy and security considerations into the architecture of any new tool. From the start, clear nontechnical language should inform users about what personal information is used, how it is stored, and with whom it is shared. Users should have the opportunity to explicitly consent to the collection of data, especially when the information is not strictly necessary for the application's core public health function. Developers should make their platforms available for third-party privacy and security audits and include opportunities for effective petition and redress for abuses. In addition, companies should avoid working with governments and private actors that perpetrate or facilitate human rights abuses.

For Civil Society

Conduct research on and raise awareness of intrusive new surveillance technologies. Civil society groups should engage in innovative initiatives that inform the public about the privacy and other human rights harms wrought by unchecked state and corporate data collection. Watchdog groups should engage in technical analysis to determine the human rights risks posed by smartphone apps, biometric surveillance, and other emerging technologies.

Utilize strategic litigation to push back against state surveillance. Civil society groups and their allies have won victories in court that limited state surveillance in Brazil, Estonia, Germany, South Africa, and the United States. They should participate in strategic litigation whenever possible, or provide friend-of-the-court filings that explain how digital surveillance can 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.

PROMOTING INTERNET FREEDOM AMID A RISE IN CYBER SOVEREIGNTY

For Policymakers

Preserve broad protections against intermediary liability. Companies should continue to benefit from safe-harbor protections for most user-generated and third-party content appearing on their platforms, in keeping with principles that have allowed for a historic blossoming of artistic expression, economic activity, and social campaigning. Policies ostensibly meant to enforce political neutrality would in practice open the door to politicized government interference and negatively impact "good Samaritan" rules that enable companies to moderate harmful content without fear of unfair legal consequences. In line with the Manila Principles, governments should work together with technical, legal, and human rights experts to establish meaningful oversight measures for technology companies, including the ability to evaluate their content moderation practices for transparency, proportionality, and the effectiveness of appeals processes.

Restrict the export of censorship and surveillance technology. Given the significant potential for abuse, trade in censorship and surveillance technologies should be restricted, particularly for end users that are known to have committed human rights violations. The United States is currently updating export control requirements for emerging technologies, foundational technologies, and items used in crime control and detection. Any final rule issued by the US government should ensure that technologies enabling monitoring, surveillance, and the interception or collection of information and communications—including systems that use machine learning, natural language processing, and deep learning—are included on the Commerce Control List and cannot be sold to countries rated Partly Free or Not Free by any Freedom House publication.

Bolster cyber diplomacy in defense of an open, free, and global internet. Diplomats should make greater efforts to push back against data localization requirements around the world, particularly in repressive countries where the human rights implications for local users are stark. In the United States, the proposed Cyber Diplomacy Act (H.R.739) would establish an Office of International Cyberspace Policy within the State Department, headed by an ambassador for cyberspace, to lead cyber diplomacy efforts. The office would be tasked with implementing a US international cyber policy that advances democratic principles and promotes an open, interoperable, and secure internet governed by a multistakeholder model. The legislation requires the inclusion of internet freedom in annual State Department country assessments and the formulation of a strategy for engaging foreign governments to develop international norms of responsible state behavior on cyber issues.

Lead by example. Freedom House research consistently shows that governments learn from one another, copying restrictive policies and actions from foreign states to implement at home. This includes less free governments that cite the actions of democracies to justify their own repressive policies. Democratic leaders should demonstrate respect for internet freedom principles by adhering to domestic legislation in line with international human rights laws and standards, and by refraining from rhetoric that undermines these standards.

For the Private Sector

Adhere to the UN Guiding Principles on Business and Human Rights and conduct human rights impact assessments for new markets, 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 provide surveillance or law enforcement equipment that is likely to be used to commit human rights violations. 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 like freedom of expression or 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.

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.

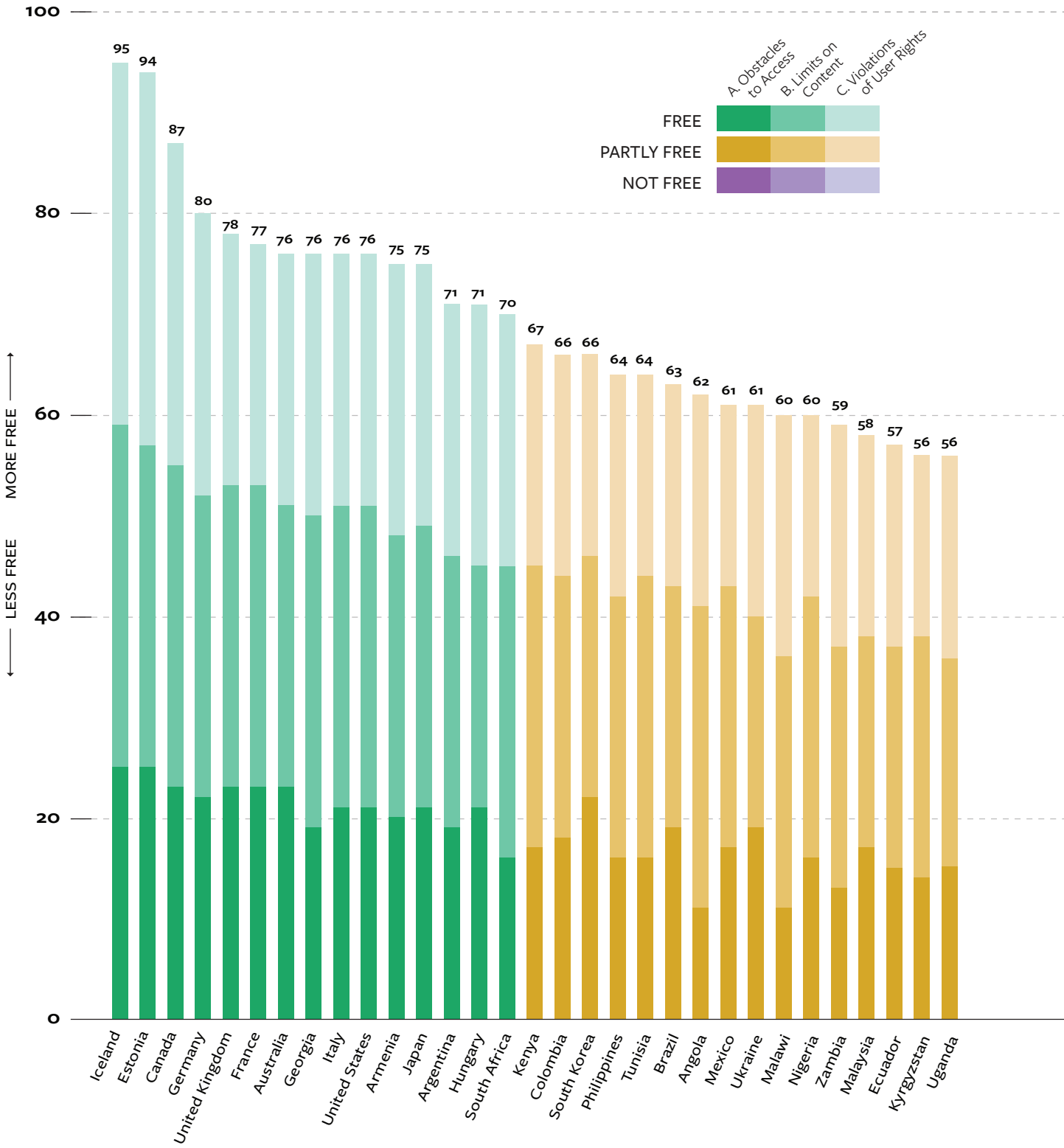
For Civil Society

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 or HTTPS browsing—derive from innovations in technical standards and product design that were effectively pushed 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.

People use their mobile phones during a rally in Minsk supporting Sviatlana Tsikhanouskaya, the opposition candidate in the deeply flawed August 2020 presidential elections. Photo credit: Nataliya Fedosenko/TASS via Getty Images.

GLOBAL RANKINGS

100 = Most Free 0 = Least Free



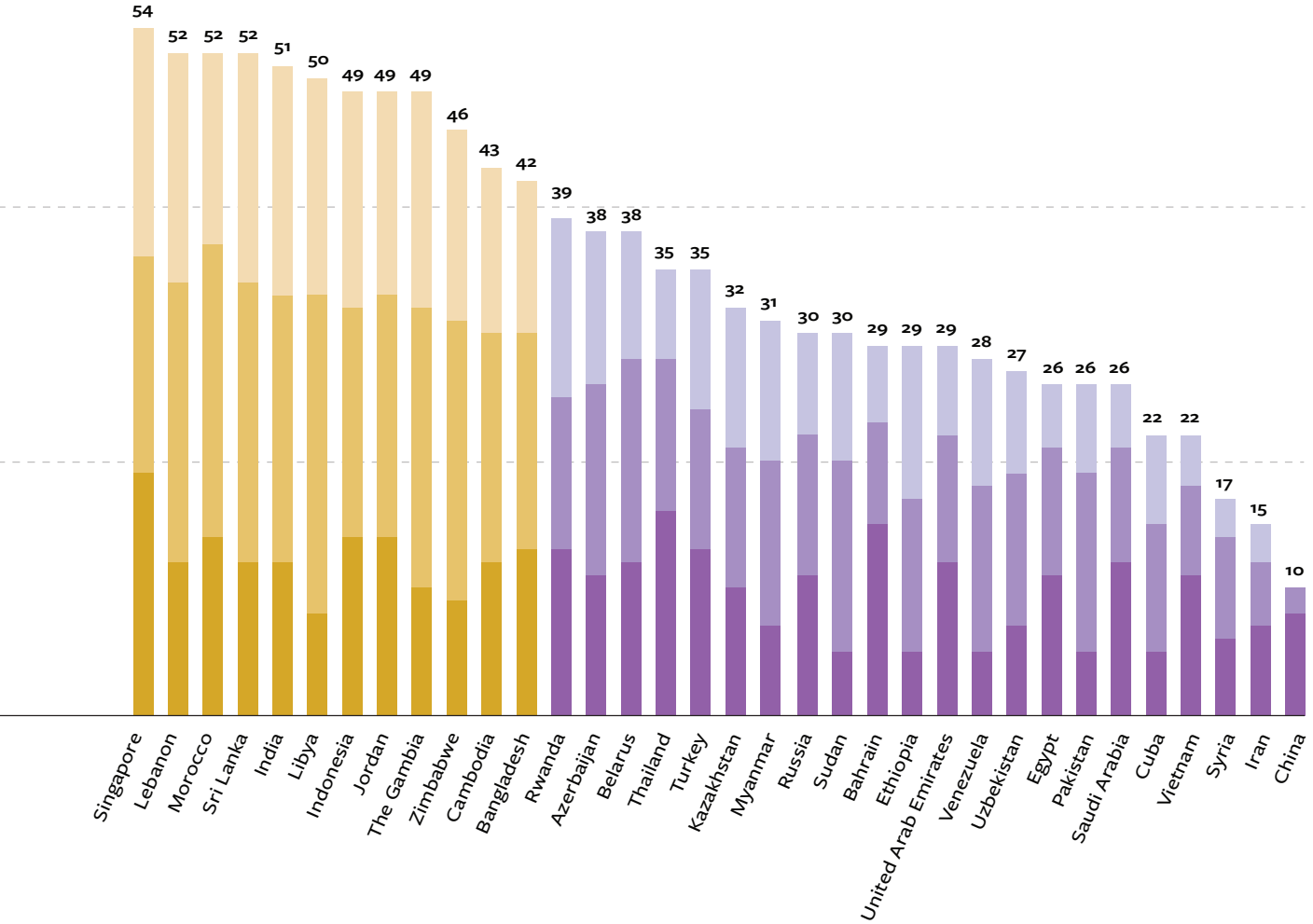
Freedom on the Net measures the level of internet freedom in 65 countries. Each country receives a numerical score from **100 (the most free)** to **0 (the least free)**, which serves as the basis for an internet freedom status designation of **FREE (100-70 points)**, **PARTLY FREE (69-40 points)**, 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.



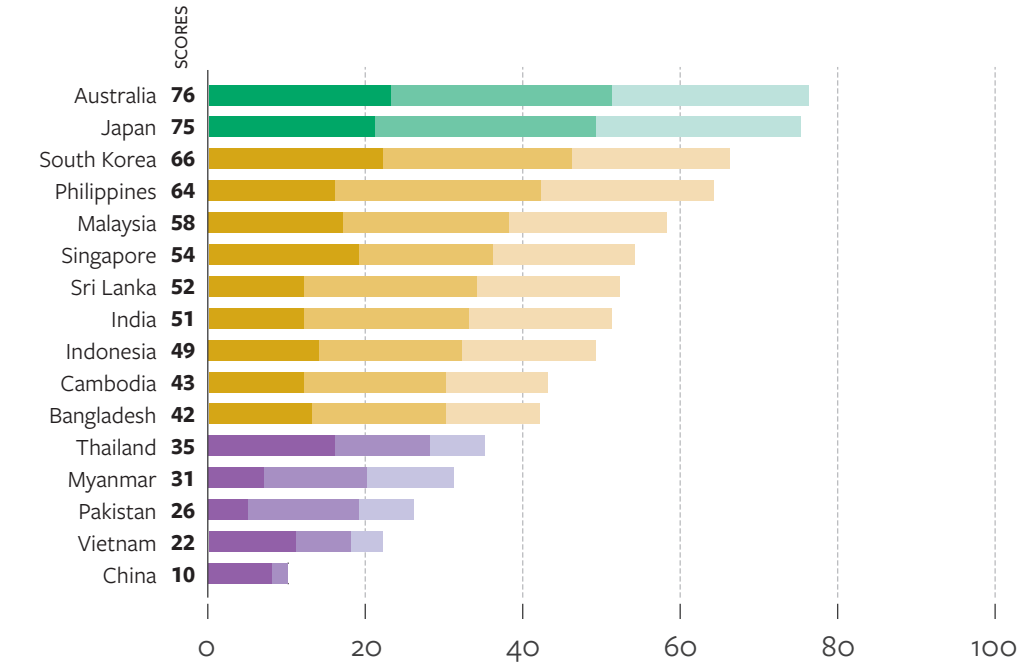
REGIONAL RANKINGS

Freedom on the Net 2020 covers 65 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

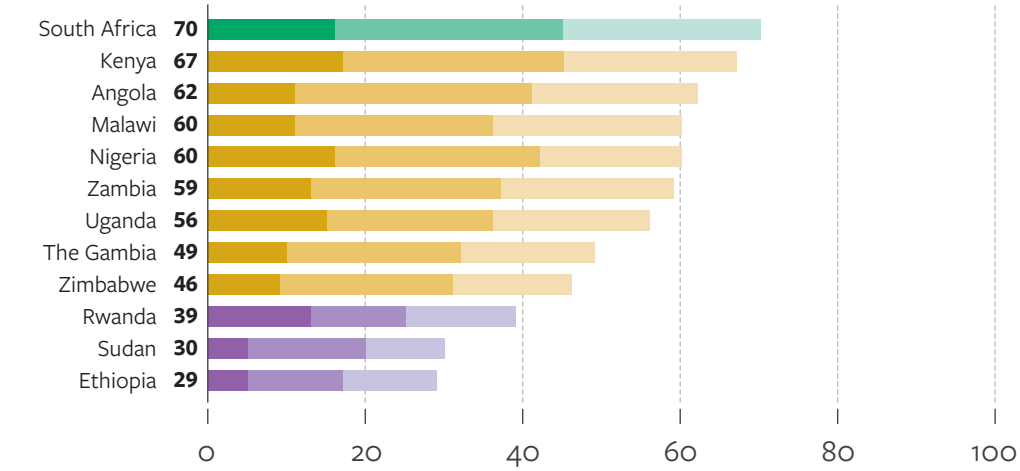
A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights

0 = Least Free
100 = Most Free

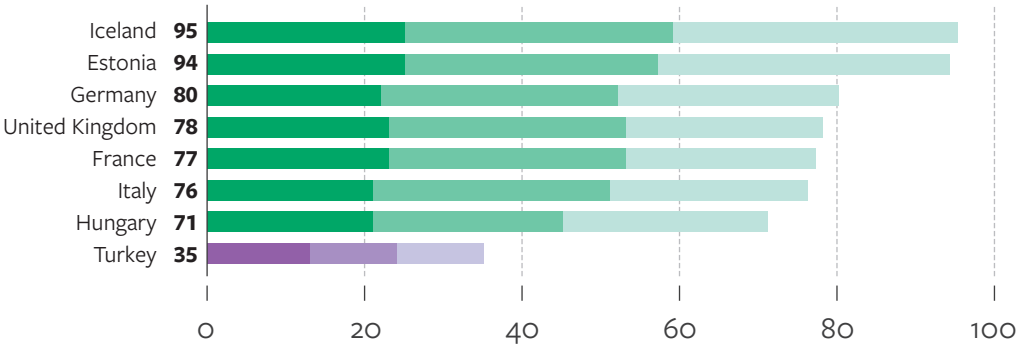
Asia-Pacific



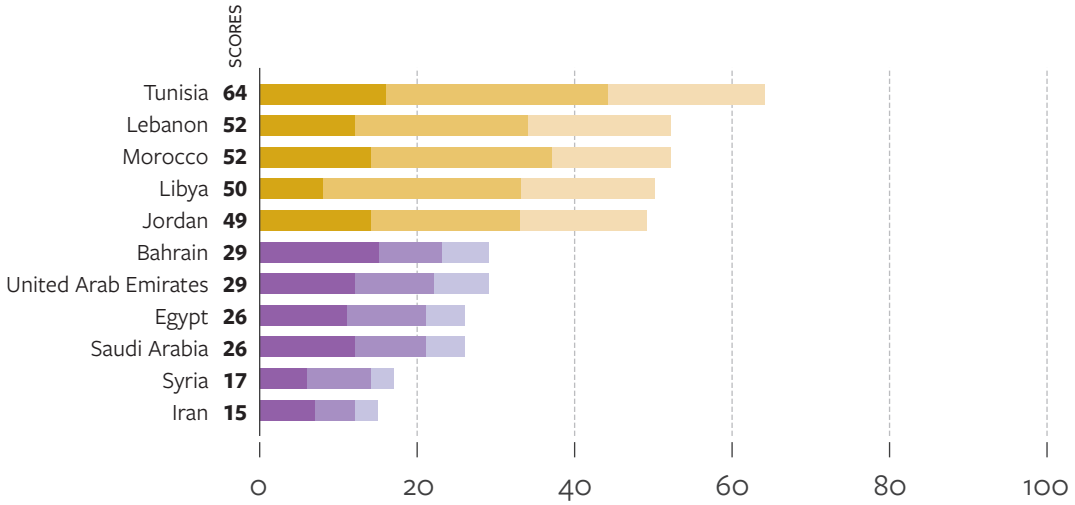
Sub-Saharan Africa



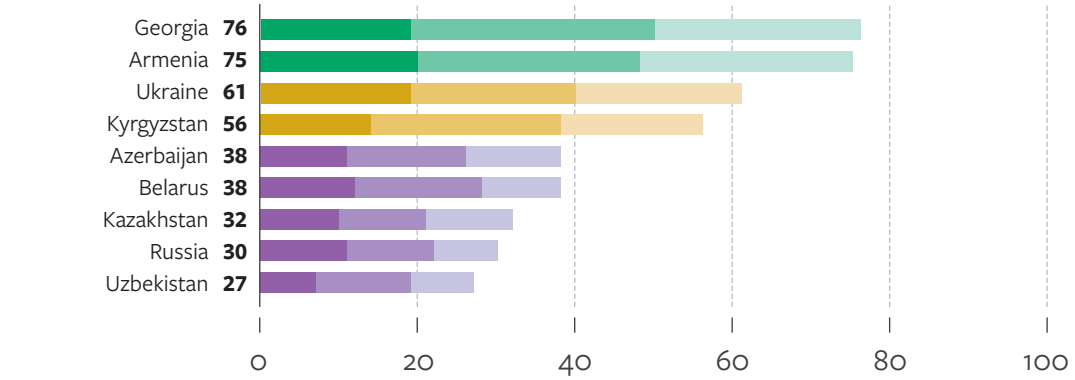
Europe



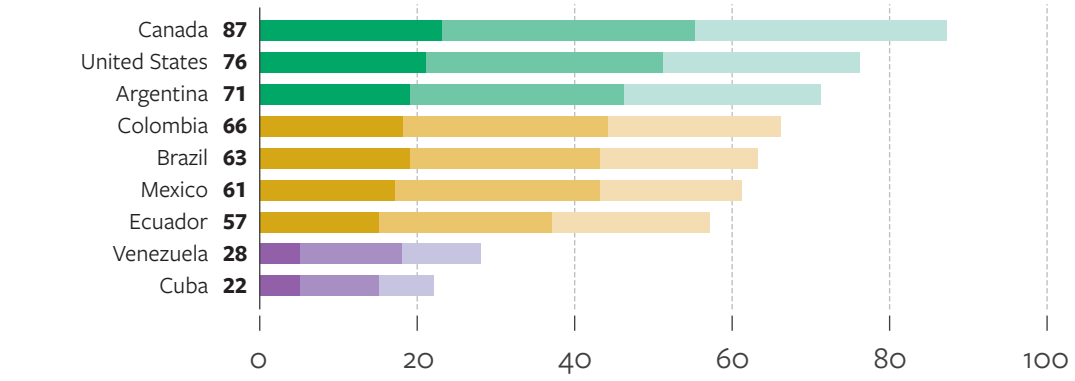
Middle East and North Africa



Eurasia



Americas



Freedom House

Freedom House is a nonprofit, nonpartisan organization that supports democratic change, monitors freedom, and advocates for democracy and human rights.

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

freedomhouse.org
facebook.com/FreedomHouseDC
@freedomhouse
@freedomonthenet
202.296.5101 | info@freedomhouse.org