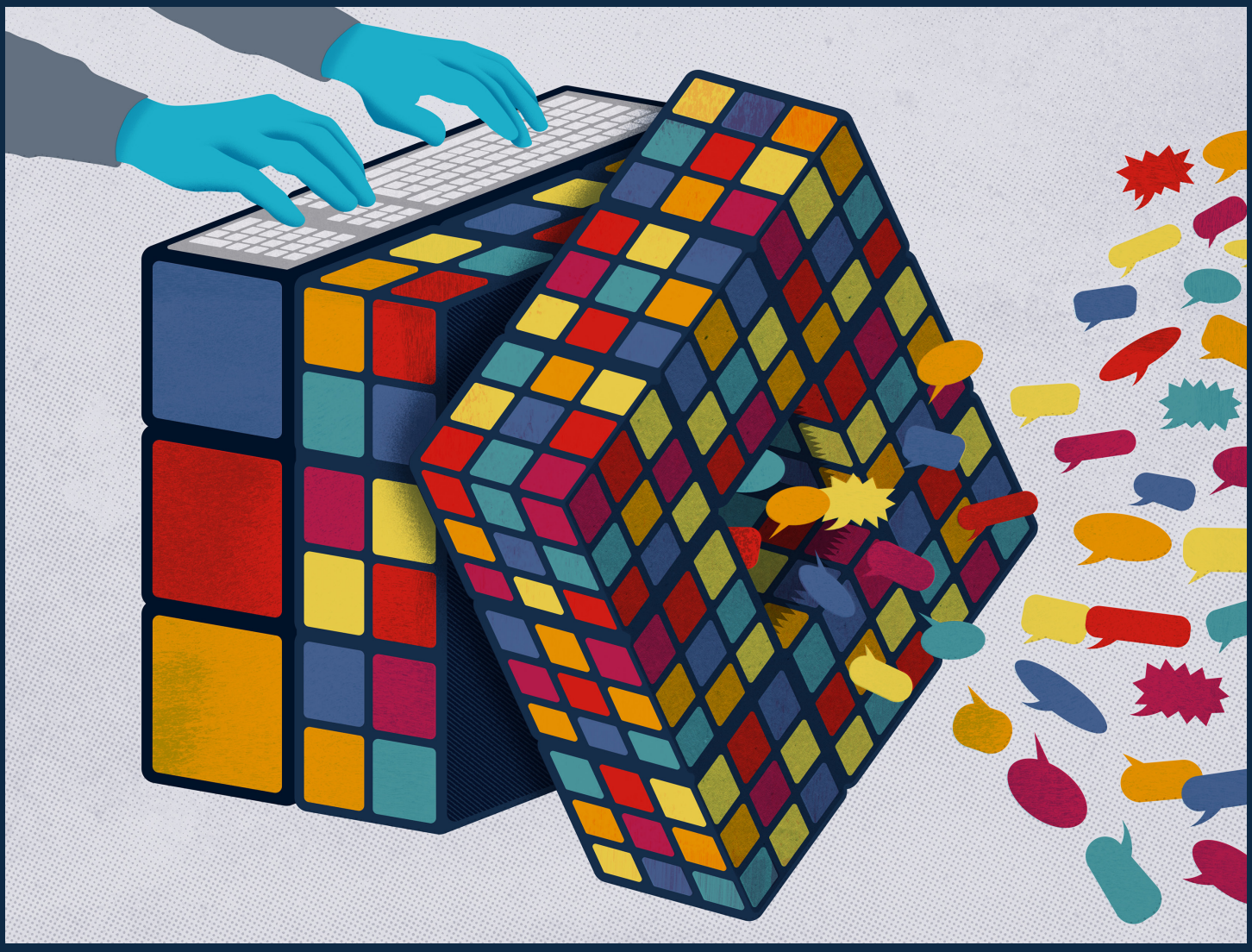
Freedom House

FREEDOM ON THE NET 2025

An Uncertain Future for the Global Internet



Highlights from Freedom House's annual report on internet freedom

FREEDOM ON THE NET 2025

TABLE OF CONTENTS

Key Findings 1

Freedom on the Net 2025: An Uncertain Future for the Global Internet ... 2

- Tracking the Global Decline 4
- Fifteen Years of Evolution in Internet Controls 8
- On the Horizon for Human Rights Online 14

Policy Recommendations 28

What We Measure 32

Checklist of Questions 33

Acknowledgements and Sources 40

TABLES, CHARTS, AND GRAPHICS

- Detained for Dissent 4
- Global Internet User Stats 6
- Internet Freedom's 15 Years of Decline 9
- The Perils and Promises of AI Sovereignty 15
- A Crisis for Online Anonymity 19
- Key Internet Controls by Country 21
- *Freedom on the Net 2025* Map 22
- Global Rankings 24
- Regional Rankings 26

This booklet is a summary of findings for the 2025 edition of *Freedom on the Net*. Summaries of developments in the 72 countries assessed in this study can be found on our website at freedomonthenet.org.

ON THE COVER

Illustration by Mitch Blunt

Key Findings

1

Global internet freedom declined for the 15th consecutive year. Of the 72 countries assessed in *Freedom on the Net 2025*, conditions deteriorated in 27, while 17 countries registered overall gains. Kenya experienced the most severe decline of the coverage period, after authorities responded to nationwide protests over tax policy in June 2024 by shutting down internet connectivity for around seven hours and arresting hundreds of protesters. Bangladesh earned the year's strongest improvement, as a student-led uprising ousted the country's repressive leadership in August 2024 and an interim government made positive reforms. China and Myanmar remained the world's worst environments for internet freedom, while Iceland held its place as the freest online environment.

2

Half of the 18 countries with an internet freedom status of Free suffered score declines during the coverage period. Only two countries in this group received improvements. People in Georgia experienced the most significant decline in the Free cohort, followed by Germany and the United States, as the ruling Georgian Dream party enacted repressive measures targeting civil society. Authorities in Germany pursued criminal prosecutions against people who criticized politicians, while threats from far-right actors further encouraged self-censorship online. In the United States, growing restrictions on civic space threatened to stifle digital activism, marked by the detention of foreign nationals for nonviolent online expression.

3

Control over online information has become an essential tool for authoritarian leaders seeking to entrench their regimes. Governments in the countries that suffered the most extreme declines over the 15 years of global deterioration in internet freedom—Egypt, Pakistan, Russia, Turkey, and Venezuela—intensified their control over the online environment in response to challenges to their rule. Authorities in these settings expanded restrictions on content, escalated surveillance of electronic communications, and imposed more severe penalties on those who expressed dissent online, particularly during protests and elections. The pattern illustrates how digital repression has proven essential for regime security in authoritarian states.

4

Online spaces are more manipulated than ever, as authorities seek to promote favored narratives and warp public discourse. Of the 21 indicators covered by *Freedom on the Net*, the one that assesses whether online sources of information are manipulated by the government or other powerful actors has undergone the most consistent global decline over the past 15 years. Information manipulation campaigns have reshaped online spaces, with common methods including paid commenters who masquerade as ordinary internet users, news sites mimicking trusted outlets, misleading content generated by artificial intelligence (AI), and prominent social media influencers who post progovernment content without clear or formal affiliation.

5

The immediate future of internet freedom will depend on the ways in which governments deploy and regulate new technologies. Governments are overseeing investments in their domestic AI industries that will shape how people interact with chatbots, synthetic media, and other AI-enabled products, with important implications for privacy and free expression in countries where safeguards are lacking. Advances in satellite-based internet connectivity are bringing many communities online, particularly in rural and war-torn areas, exposing satellite service providers to government pressure regarding surveillance and censorship. Online anonymity, an essential enabler for freedom of expression, is entering a period of crisis as policymakers in free and autocratic countries alike mandate the use of identity verification technology for certain websites or platforms, motivated in some cases by the legitimate aim of protecting children.

Freedom on the Net 2025: An Uncertain Future for the Global Internet

By Kian Vesteinsson and Grant Baker

The internet is more controlled and more manipulated today than ever before. Global internet freedom declined for the 15th consecutive year in 2025, as authoritarian governments employed censorship and offline repression to quash protests that were organized online, and people in democracies faced an escalation in constraints on digital expression.

When the *Freedom on the Net* project was launched in 2011, following a 2009 pilot, there was widespread optimism about the power of information technology to support prodemocracy movements and drive progress for human rights. These hopes were buoyed by the prominent role played by online platforms in Iran's Green Movement and the Arab Spring that followed. From the outset, however, it was apparent that governments could use the same digital technologies to smother dissent and shape online narratives in their favor.

During this report's coverage period, from June 2024 to May 2025, conditions deteriorated in 27 of the 72 countries assessed, while 17 countries registered overall gains. The year's largest decline occurred in Kenya, followed by Venezuela and Georgia. China and Myanmar remained the world's worst environments for internet freedom.

The immediate future of internet freedom will depend on how governments deploy incentives for and controls over the next wave of technological innovation.

Bangladesh earned the largest improvement, while Iceland retained its status as the freest online environment, followed by Estonia.

Fifteen years of *Freedom on the Net* analysis shows that the internet has transformed the ways in which state authorities and other powerful actors assert control over information. Authoritarian rulers have deployed tools of digital repression to strengthen their hold on power, particularly in response to protests or elections that challenge their rule, driving the most precipitous cumulative score declines recorded by the report. And in countries across the democratic spectrum, from the worst autocracies to some of the world's freest societies, political leaders have sought to manipulate online narratives through increasingly sophisticated methods, often attempting to shape the information space without overt censorship.

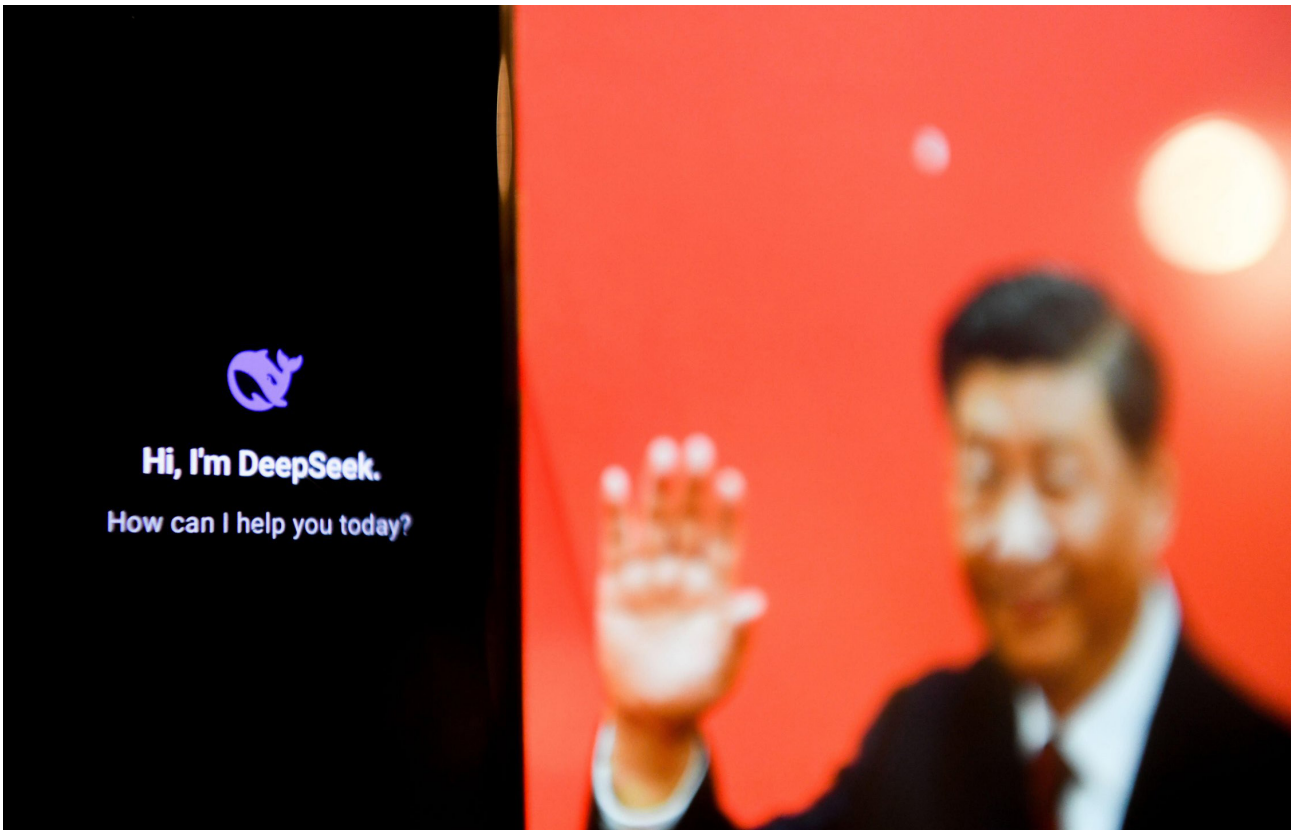
The immediate future of internet freedom will depend on how governments deploy incentives for and controls over the next wave of technological innovation. Governments around the world are already ramping up their development of AI ecosystems, pouring huge investments into cloud-computing infrastructure and natural-language and reasoning models. Innovations in satellite-based connectivity will change how people access the internet, while the rise of technical measures to verify the age and identity of people using the internet will dramatically alter the online experience. Freedom of expression, access to information, and privacy should be among the values that guide both regulation and innovation.

Those working to safeguard internet freedom face new headwinds, however. The US government's decision to dismantle its foreign aid institutions resulted in the

termination of its support for internet freedom programming, a long-standing priority across multiple Republican Party and Democratic Party administrations. The cuts entailed the cessation of funding to experts developing anticensorship technology and encrypted communication tools, to people working on human rights issues in the world's least free environments, and to organizations that assisted journalists, activists, and others under threat for the content they posted online. (Freedom House was among the organizations that were materially affected by the freeze in US foreign assistance, which included the removal of funding for *Freedom on the Net* and our broader emergency support programs.) The United States has long served as a leading advocate of global internet freedom, and its withdrawal from the vanguard leaves a significant gap.

About this report: This is the 15th edition of *Freedom on the Net*, an annual study of human rights online. The project assesses internet freedom in 72 countries, accounting for 89 percent of the world's internet users. This report covers developments between June 2024 and May 2025. The report uses a standard methodology to determine each country's internet freedom score on a 100-point scale, with 21 separate indicators pertaining to obstacles to access, limits on content, and violations of user rights. The FOTN website features key developments and data on each country's conditions.

Fifteen consecutive years of decline should stir alarm among supporters of internet freedom and galvanize remedial efforts in the years to come. Halting and reversing the negative trend will require coordinated action by like-minded allies from government, the private sector, and civil society. As emerging technologies begin to affect the exercise of human rights online, these partners must establish safeguards for free expression and privacy to ensure that any technical innovation leads to improvements for global internet freedom.



Chinese President Xi Jinping depicted alongside the DeepSeek AI application. Governments around the world are ramping up their development of "sovereign AI" ecosystems, pouring investments into domestically based cloud infrastructure and AI models. (*Photo credit: SOPA Images Limited*)

Tracking the Global Decline

State responses to mass protests, deepening technical censorship, and threats to free speech in democracies fueled the 15th consecutive year of decline in internet freedom. People in at least 57 of the 72 countries covered by *Freedom on the Net 2025* were arrested or imprisoned for online expression on social, political, or religious topics during the coverage period—a record high. In May 2025, a Saudi Arabian court sentenced British citizen Ahmad al-Doush to 10 years in prison, reportedly over a deleted 2018 social media post about Sudan and his association with an exiled Saudi critic, though the sentence was reduced to 8 years in June 2025, after the coverage period. In October 2024, a Belarusian court sentenced Andrei Parotnikau, a political analyst and blogger, to 10 years in prison on trumped-up charges including treason and promotion of extremist activities.

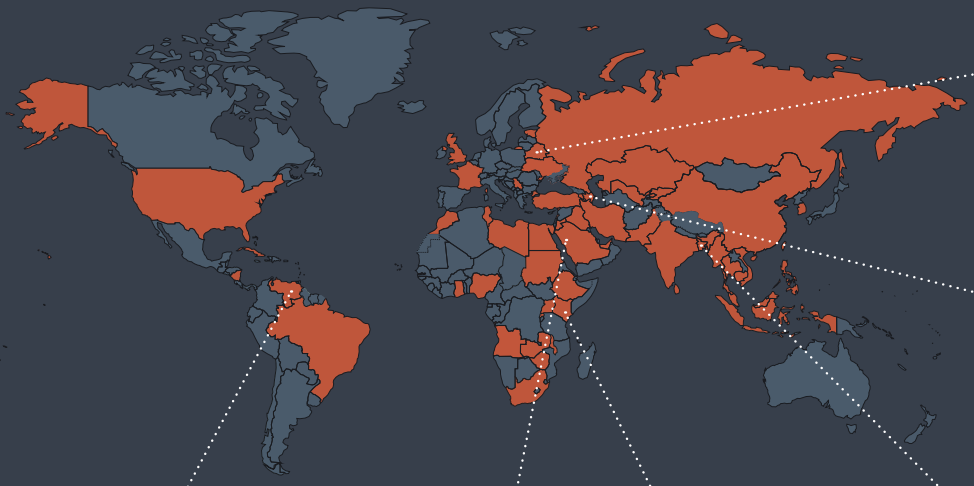
A year of mass mobilization

Protests and large-scale uprisings drove some of the year's most significant developments, as governments engaged in digital repression to thwart communication about acts of dissent. Across the board, authorities arrested online critics and protest organizers. In the more severe cases, governments pursued wholesale restrictions on internet access.

Kenyan authorities carried out a violent crackdown, contributing to the year's largest score decline, after people mobilized nationwide and online in June 2024 to protest new tax policies and perceived economic mismanagement. The government imposed an approximately seven-hour internet shutdown—the first such connectivity restriction reported

Detained for Dissent

From the worst autocracies to some of the world's freest societies, people were arrested or imprisoned for online expression on social, political, and religious topics. These are some of the most severe cases.



Belarus

A court sentenced political blogger Andrei Parotnikau to 10 years in prison on trumped-up charges in October 2024.

Azerbaijan

In February 2025, authorities sentenced Matlab Baghirov, who ran two religious online media outlets, to 12 years in prison on politicized charges.

Venezuela

In February 2025, opposition activist Nelson Piñero was sentenced to 15 years in prison for criticizing Nicolás Maduro's government on social media.

Saudi Arabia

In May 2025, a court sentenced visiting British national Ahmed al-Doush to 10 years in prison, reportedly over political commentary posted on social media in 2018.

Kenya

Authorities arrested hundreds of people who had mobilized nationwide and over social media during June 2024 protests.

Bangladesh

Ahead of the ouster of the repressive Awami League government in August 2024, security forces carried out mass arrests and violence against demonstrators.

Certain territories that are assessed separately in Freedom House's *Freedom in the World* report are excluded from the relevant country assessments in Freedom on the Net, as conditions in territories differ significantly from those in the rest of the country.

in Kenya—and arrested hundreds of protesters. Arrests and disappearances of online activists and critics continued throughout the coverage period, and some of the detainees reported abuse in custody.

The Venezuelan government employed a barrage of internet controls ahead of the July 2024 presidential election and in response to mass protests that followed the National Electoral Council's unsubstantiated announcement that authoritarian incumbent Nicolás Maduro won the election, prompting the second-largest decline in *Freedom on the Net 2025*. The government blocked wide swathes of the internet—including social media and communications platforms, websites of news outlets and civil society groups, and anticensorship tools—as part of a broader effort to limit online discussion and mobilization about serious irregularities in the vote count. Authorities sought to imprison those who challenged the official narrative, detaining digital journalists and forcibly disappearing people who criticized the government online.

The Serbian government's response to student-led protests caused that country's internet freedom status to change from Free to Partly Free. When people took to the streets across the country to call for justice and transparency following the deadly collapse of a train station canopy in Novi Sad in November 2024, authorities detained individuals who spoke out in support of the protests online and employed Cellebrite technology to search the phones of journalists and activists.

Protests and large-scale uprisings drove some of the year's most significant developments, as governments engaged in digital repression to thwart communication about acts of dissent.

Bangladesh received the year's largest score improvement after a student-led uprising culminated in the ouster of longtime Prime Minister Sheikh Hasina and her repressive Awami League (AL) government in August 2024. In July of that year, the AL government restricted access to mobile internet service for 11 days and blocked a host of social media platforms, even as protesters endured brutal state violence. Conditions improved somewhat after Hasina fled the country. While perceived supporters of the AL faced a concerning

Serbians mobilized nationwide to protest corruption following the deadly collapse of a train station canopy in November 2024. The government detained people who supported the protests online, causing Serbia's internet freedom status to change from Free to Partly Free. (*Photo credit: Mirko Kuzmanovic*)

pattern of retaliation, an interim government carried out some small-scale reforms, and the general opening of democratic space presented a rare opportunity for the advancement of internet freedom.

Authoritarians impose deeper censorship

Some of the world's most repressive governments expanded their technical censorship efforts during the coverage period. These measures were often accompanied by the arrest and intimidation of online activists, as well as legal provisions that undermined people's online privacy.

Censorship intensified in China and Myanmar, which remained the world's worst environments for internet freedom. Chinese authorities continued to develop the country's censorship infrastructure, with research from the coverage period finding that provincial-level authorities were vigorously blocking online content—sometimes at a scale 10 times that of the national-level system known as the Great Firewall. Leaked documents confirmed that a Chinese company had exported the technology that supports the Great Firewall to facilitate government censorship in other countries, including Myanmar, where the military regime has worked to crush dissent since a 2021 coup. Myanmar authorities also enacted a cybersecurity law in January 2025 that restricted the operation of anticensorship tools in the country and codified the regime's de facto censorship practices.

Authorities in Russia ramped up efforts to further isolate Russians from the global internet throughout the coverage period. In the summer of 2024, the government blocked the end-to-end encrypted messaging application Signal and began throttling YouTube, one of the few major social media platforms that had remained unblocked since Moscow's full-scale invasion of Ukraine in 2022. Later in the year, the government restricted access to websites employing Cloudflare services with the Encrypted Client Hello protocol, which helps safeguard user privacy by concealing information about users' browsing activity. In May 2025, the government began sporadically shutting down access to mobile internet service across the country, citing concerns about attacks from Ukraine.

In Nicaragua, the authoritarian regime of President Daniel Ortega revoked the .ni domain registrations of independent news websites, the first technical censorship recorded in

GLOBAL INTERNET USER STATS

Over **5.5 billion** people have access to the internet.

According to Freedom House estimates:

81% live in countries where individuals were arrested or imprisoned for posting content on political, social, or religious issues.

70% live in countries where individuals were attacked or killed for their online activities.

70% live in countries where authorities deployed progovernment commentators to manipulate online discussions.

69% live in countries where political, social, or religious content was blocked online.

61% live in countries where access to social media platforms was temporarily or permanently restricted.

52% live in countries where authorities disconnected internet or mobile networks, often for political reasons.

a multiyear crackdown on press freedom. The country's internet freedom status was downgraded from Partly Free to Not Free as the government forced online media outlets to cease operations. Moreover, amendments to the cybercrime law that were adopted in September 2024 increased criminal penalties for spreading information that the government deems to be false and empowered authorities to obtain user data from telecommunications firms without a court order.

Pressure in democracies

In a concerning sign, half of the 18 countries with an internet freedom status of Free suffered score declines during the coverage period, while only two received improvements. People in Georgia experienced the most significant decline among these countries, followed by Germany and the United States.

In Georgia, which tied for the second-largest decline in *Freedom on the Net 2025*, the ruling Georgian Dream party continued its campaign against civil society after a new law on "transparency of foreign influence"—which compelled civil society organizations and online media outlets that receive foreign funding to register with the government—took effect in August 2024. Ahead of the October 2024 elections, law enforcement agencies conducted raids on two Atlantic Council researchers who had studied online influence operations in Georgia. In February 2025, Georgia's parliament passed amendments to the Law on Assemblies and Demonstrations that introduced criminal penalties of up to 45 days in prison for insulting public officials. The amendments were then used to charge people who criticized the government online after the coverage period.

The German government, led by the Christian Democratic Union (CDU) and Christian Social Union (CSU) coalition since the February 2025 elections, has pursued criminal prosecutions against people who made memes about politicians, invoking laws against insult and hate speech. Self-censorship also increased because of intimidation by far-right actors against journalists, professional and legal reprisals against people who criticized the Israeli government online, and concerns about rising antisemitic and anti-Muslim hate speech as well as a reported increase in offline violence and threats against both Jews and Muslims. Meanwhile, hackers with ties to the Russian state launched cyberattacks against the CDU ahead of European Parliament elections in June 2024.

> The United States retained its overall status of Free, though growing restrictions on civic space drove a significant decline.

While the United States retained its overall status of Free, growing restrictions on civic space drove the decline in its score. The administration of President Donald Trump detained several foreign nationals for one to two months after revoking their visas over nonviolent online expression, as part of a larger program to arrest and deport noncitizens. The Federal Communications Commission and the Federal Trade Commission threatened or carried out politicized investigations into civil society organizations and media and technology companies, often focusing on their content moderation, editorial decision-making, or forms of speech that are protected by the US Constitution's First Amendment. More broadly, the administration's actions have chilled the atmosphere for digital activism.

Modest improvements

Some gains in internet freedom were recorded in countries that ranked Partly Free or Not Free in *Freedom on the Net*, primarily because their governments imposed less severe restrictions than in the previous coverage period. Ethiopia and Kazakhstan received score improvements after authorities imposed less extensive internet shutdowns than in the previous year and made progress in diversifying their domestic telecommunications sectors. Angola and Zimbabwe experienced marginal gains as government-linked efforts to manipulate online information appeared less common during the coverage period. Around the world, meanwhile, countries continued to expand overall access to the internet. The spread of internet services and increased affordability brought improvements in Morocco, the Philippines, and Uzbekistan. Although such incremental changes are welcome, the governments in question have track records of digital repression and still lack legal and institutional safeguards that would protect free expression and privacy over the long term.

Fifteen Years of Evolution in Internet Controls

The internet has transformed how authorities assert control over information in every political environment, from the world's most repressive autocracies to robust electoral democracies. Over the past 15 years of *Freedom on the Net* research, antidemocratic leaders have employed a dizzying array of increasingly sophisticated legal and technical measures to influence and dominate the online landscape, particularly in response to challenges to their rule. Meanwhile, social media platforms that host user-generated content have come to define people's experience on the internet, and campaigns to manipulate the material on these platforms have become more pervasive and refined. Manipulation campaigns often serve as a means for authorities to shape narratives on the internet without relying on more overt censorship or repression.

Authoritarians refine digital restrictions

Over the past decade and a half, authoritarian regimes have deployed increasingly advanced and widespread measures to control online information in an effort to stay in power. In response to mass protests, political activism, or other challenges to their rule, authoritarian leaders worked to dominate digital environments that were comparatively open when *Freedom on the Net* analysis began in 2011. From technical censorship to draconian criminal penalties for online dissent, their combined repressive measures drove the sharpest long-term declines in internet freedom among the 72 countries covered by the report. Conditions in some of these authoritarian states now approach those in China, where the Chinese Communist Party has long set the standard for digital authoritarianism, and in Iran, where the regime has sought to establish a similar level of censorship and isolation.

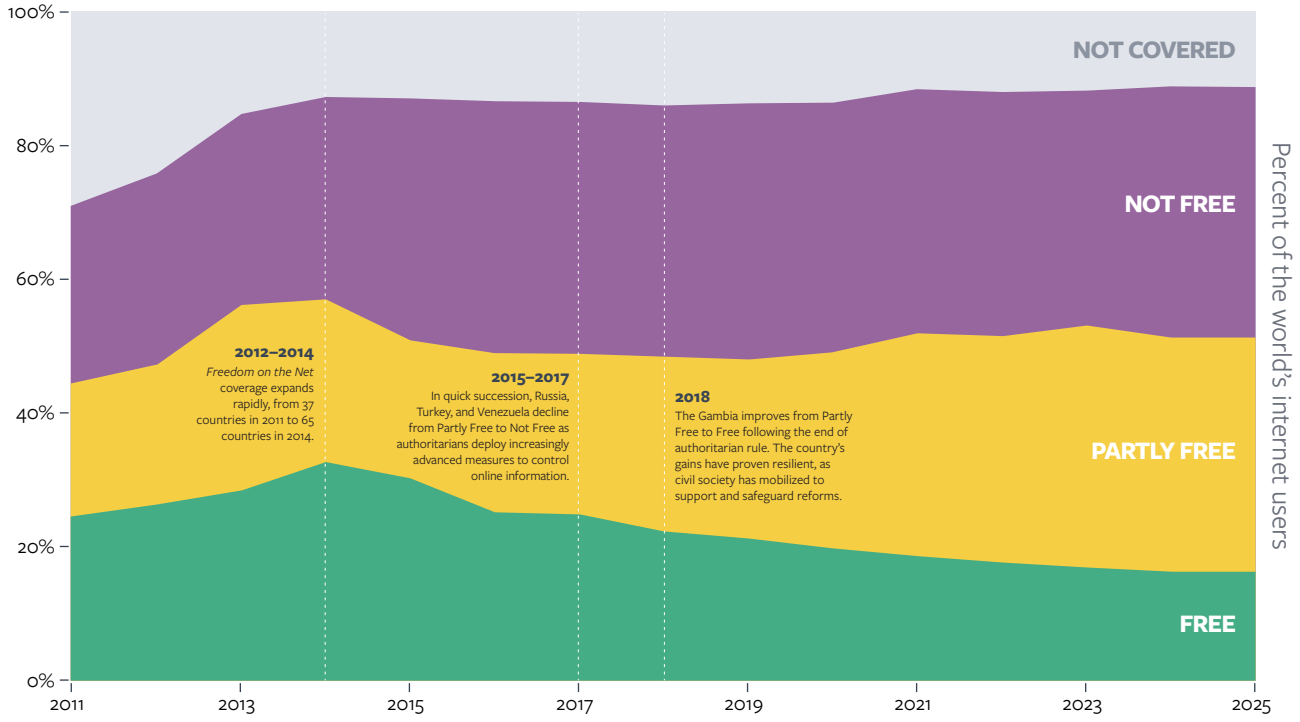
In response to mass protests, political activism, or other challenges to their rule, authoritarian leaders worked to dominate digital environments.

In Russia, which underwent the steepest 15-year decline in internet freedom, President Vladimir Putin has attempted to carve out a sanitized domestic internet while crushing dissent. In the aftermath of widespread antigovernment protests between 2011 and 2013 and the 2014 invasion of Ukraine, Russian authorities laid the groundwork for a "sovereign internet," a technical and legal project to disconnect Russia from the global network. Early restrictions on the internet were not always effective, leaving space for opposition figures, like Aleksey Navalny and his Anti-Corruption Foundation, to organize and advocate online. Even in 2018, the Kremlin was technically unable to follow through on its declared blocking of Telegram. However, new censorship technology developed under the 2019 Sovereign Internet Law and subsequent legislation, which forced popular platforms to comply with Russian law, granted Putin greater practical control over the online space. By the beginning of Moscow's full-scale invasion of Ukraine in 2022, the new censorship model was demonstrably more effective, as the regime blocked access to international social media platforms, independent news outlets, and human rights organizations.

Since Egyptian President Abdel Fattah al-Sisi came to power in a 2013 coup, his government has also developed increasingly complex technical controls aimed at silencing his opponents. During the country's 2011 revolution, then-President Hosni Mubarak infamously ordered a shutdown of the internet for five days and deployed security forces against protesters. President Sisi's government has since carried out widespread arrests of dissidents and developed a more targeted censorship and surveillance apparatus, rarely imposing wholesale shutdowns. In 2017, the government deployed deep packet inspection technology to block websites, restricting access

INTERNET FREEDOM'S 15 YEARS OF DECLINE

As of 2025, a lower proportion of the world's internet users live in countries ranked Free by *Freedom on the Net* than ever before.

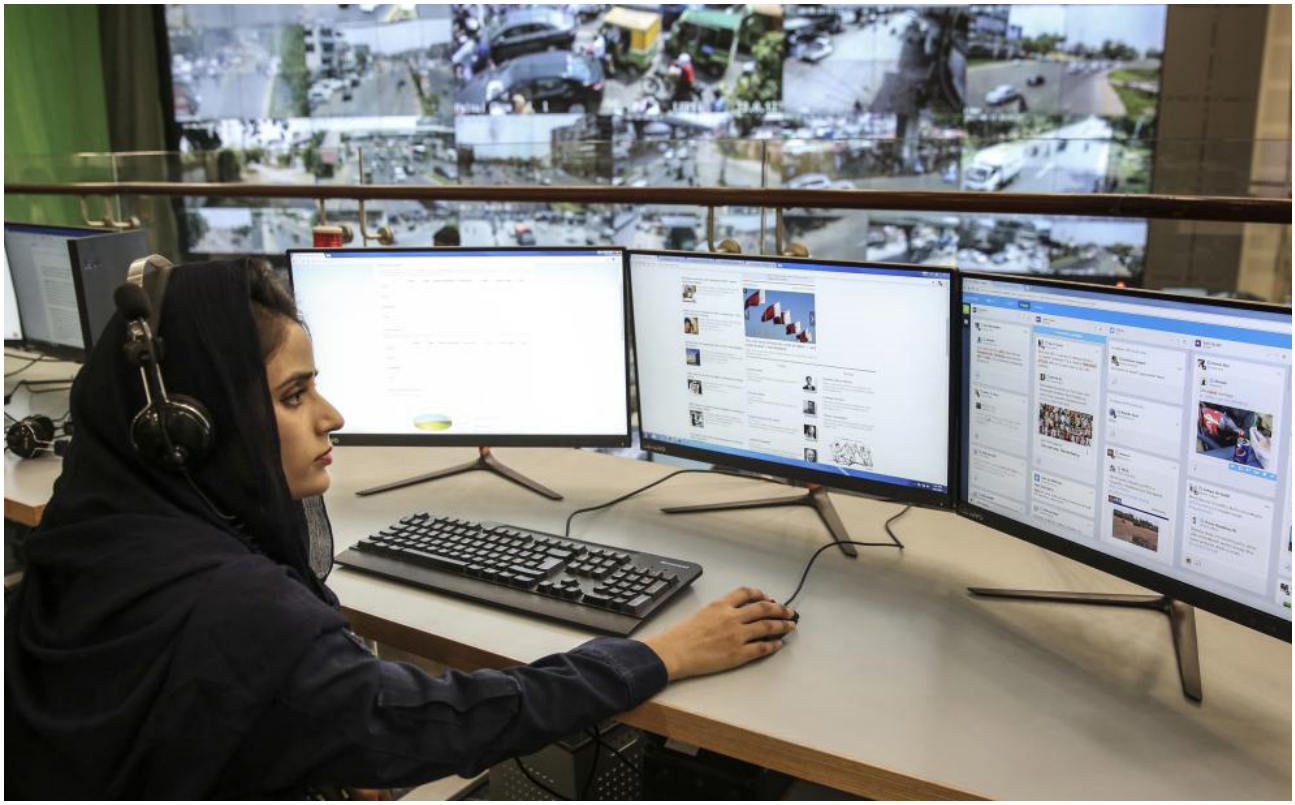


to some 600 proxy servers, news outlets, and other sites in a three-year period. The Sisi regime has also surveilled prominent opposition politicians with the aid of spyware tools that enable covert access to infected devices, according to investigations by the Canada-based research group Citizen Lab.

Authorities in Turkey have consolidated an expansive censorship system over the past 15 years, spurred by the 2013 Gezi Park protests, which grew into a nationwide movement organized in part on social media platforms. The protests illuminated how people could use social media to sidestep conventional press censorship. In their aftermath, law enforcement officials escalated efforts to prosecute online journalists and digital activists. Recep Tayyip Erdoğan, then the prime minister and since 2014 the president of Turkey, pressed criminal charges against dozens of people for online insult after the protests, and continued to do so in the decade that followed. Erdoğan's government has relied on blunt censorship measures, like website blocking and throttling of social media, and enacted new laws to compel online media outlets and platforms to remove content that is critical of the political leadership.

Venezuelan authorities have imposed harsher digital controls in the face of widespread discontent over the country's interlocking economic and political crises. When Maduro assumed power in 2013, censorship of the conventional media had not yet extended to the internet, enabling a diverse online environment. The regime soon introduced censorship measures, including internet shutdowns and blocking of independent media sites, as a means of curtailing dissent. Some of the worst declines in the country's internet freedom have coincided with its elections, which were rigged to ensure victory for Maduro and his allies. Venezuelans have responded by protesting in the streets and on digital platforms, triggering brutal state violence, as in the aftermath of the July 2024 balloting described above.

Pakistani authorities have imposed more stringent digital censorship measures to maintain the military establishment's grip on power and its influence over the country's elections and civilian governments. The government secured passage of an expansive censorship law in 2016 that gave state agencies greater authority to silence dissent and activism, and installed



A Pakistani police officer monitors social media in 2017. Over the 15 years of *Freedom on the Net* analysis, Pakistani authorities have expanded their legal and technical capacity to carry out censorship and surveillance. (*Photo credit: Asad Zaidi/Bloomberg via Getty Images*)

a website-blocking system to translate that legal authority into technical control. In the decade that followed, the government repeatedly extended the remit of the 2016 law to wider swathes of online speech, particularly social media discussions, and bolstered its own technical capacity for censorship. During the coverage period, Pakistani authorities criminalized the sharing of what they deemed to be false information and deployed Chinese website-blocking technology as part of a barrage of censorship measures aimed at curtailing the reach of former Prime Minister Imran Khan and supporters of his Pakistan Tehreek-e-Insaf party, who alleged that the military had engineered his removal from power in 2022.

Blunt censorship measures and arrests for online speech have been integral to authoritarians' efforts to dominate the information space. But these regimes have also turned to more subtle measures, such as the covert manipulation of online discussions to promote favorable narratives. That tactic has become increasingly common across the global internet, influencing autocracies and democracies alike over the past 15 years.

Information manipulation reshapes the internet

State-backed manipulation efforts have drastically altered the information available online in many countries and on the internet as a whole. Over 15 years of *Freedom on the Net* monitoring, the indicator that evaluates whether online sources of information are manipulated by the government or other powerful actors has declined more than any other of the 21 indicators tracked by the project. Its deterioration has been driven primarily by campaigns that sought to manipulate online information in the government's favor through paid social media commenters, networks of automated accounts, or other means, and by efforts to compel online media outlets to align their reporting with the government's interests. While many of these campaigns are orchestrated by domestic political actors, they obfuscate their origin and misrepresent content as authentic and organic. Their cumulative effect has been to undermine public access to reliable information and prompt the passage of poorly crafted anti-misinformation laws that harm freedom of expression.

FRAGILE GAINS IN INTERNET FREEDOM

During the 15 consecutive years of decline in global internet freedom, the largest gains in individual countries have also been among the most fragile. Moments of democratic opening facilitated significant improvements for free expression and privacy in Belarus, Ethiopia, Myanmar, and Sudan over the history of the *Freedom on the Net* report. But these improvements were all precarious, ultimately reversed by authoritarian leaders who tightened internet controls.

Some past gains that still stand today are coming under threat. Tunisia secured the largest cumulative improvement in the index following the 2011 revolution that ousted dictator Zine el-Abidine Ben Ali. Its long-term achievements are now in peril, as President Kaïs Saïed has overseen growing repression since he seized extraordinary powers in 2021. Internet freedom conditions also improved in Georgia, in tandem with a democratic change in leadership in 2012–13. More recently, however, the Georgian government has sought to centralize power and crush dissent. In contrast, gains in The Gambia following the 2017 ouster of authoritarian ruler Yahya Jammeh remain secure, as the country's civil society has mobilized to support and safeguard reforms.

Whether they have proven fragile or enduring, these historic improvements are an important reminder that it is possible to halt and recover from the 15 years of global decline. Previous Freedom House research has found that the factors behind improvements in internet freedom vary from country to country, but that independent civil society activity is a consistent driver of rights-respecting change. Reversing the decline will require global collaboration among democratic governments, the private sector, and expert bodies; strong investment in independent civil society and news media in vulnerable countries; and a sustained commitment to fundamental rights in the years ahead.

When this project began, manipulation of online information relied mostly on manual effort, with authorities paying largely anonymous online commenters en masse to spew progovernment talking points and disparage critics. In 2011, troll accounts posted in support of Bahrain's government, regularly criticizing people who backed widespread protests calling for political reform; Bahraini activists identified the accounts as likely linked to the government. A government-funded public relations agency also created online personas of nonexistent journalists to share government propaganda. In Malaysia, ahead of the 2012 parliamentary elections, the ruling Barisan Nasional coalition deployed a "cyber army" to spread falsehoods about an opposition candidate's family on social media. In 2014, the Ethiopian government secretly paid bloggers to post progovernment articles and refute criticism of the government across social media.

Over time, social media platforms dedicated more resources to identifying state-backed influence operations, including by updating their terms-of-service provisions regarding state manipulation, hiring teams to address the problem, and bolstering their relationships with academic and civil society researchers who focused on information campaigns. These changes played out unevenly around the globe, with companies initially prioritizing markets in the United States and Europe, in part because of scrutiny from their respective governments regarding foreign influence operations. Moreover, the platforms' policy shifts prompted complaints from people who claimed that their legitimate content had

> State-backed manipulation efforts have undermined access to reliable information and prompted the passage of poorly crafted laws that harm freedom of expression.

been removed. And even as global social media platforms enhanced their efforts to identify and remove state-backed manipulation operations, the perpetrators were adopting new tactics and migrating to other platforms.

The rise of private chat-based platforms and increasing adoption of end-to-end encrypted messaging have made manipulation campaigns more difficult to detect and counter. Brazilian researchers uncovered a sophisticated network that was manipulating online narratives on behalf of former President Jair Bolsonaro, in part by laundering assertions from Bolsonaro and his allies through influencers and media outlets across WhatsApp, Telegram, YouTube, and other platforms, so that they passed as authentic expressions of support. The reach of this network enabled the Bolsonaro camp to shape online discussion in his favor during moments of political crisis, such as the aftermath of the January 2023 riots in Brasília.

AI innovation has facilitated the automation of influence operations, lowering their cost and increasing their efficiency. Ahead of the December 2024 presidential election in Ghana, a network of automated "bot" accounts spread messages written with the AI service ChatGPT on several social media platforms, with the aim of promoting the incumbent New Patriotic Party, according to disclosures by OpenAI, the developer of ChatGPT. When tensions between India and Pakistan escalated in the aftermath of a terrorist attack in Kashmir in April 2025, government-linked influencers and commenters in both countries posted waves of inflammatory and escalatory AI-generated content, drowning out reliable sources of news and information.

Content manipulation campaigns increasingly use technical tricks to masquerade as trusted sources, particularly by mimicking the names, mastheads, and formats of established

People in the Philippines cast their votes in May 2025 elections. Particularly during election periods, progovernment influencers paid through an opaque network of public relations firms have been integral to shaping public opinion in the Philippines. (*Photo credit: Ryan Eduard Benaid/ NurPhoto via Getty Images*)

news websites. In a December 2024 report, Meta stated that most of the influence operations it had removed from its platforms in the past year had redirected people to such misleading websites. In early 2024, an influence operation linked to Bangladesh's then-ruling AL party posted content on a number of social media platforms, often imitating news sites and redirecting targets to pages that denigrated the opposition. In October 2024, Singaporean researchers identified a shadowy network of news sites disguised as familiar outlets that were all reportedly registered to a little-known public relations agency; the sites posted news content that appeared to parrot Chinese state media. The imitation news sites used in manipulation campaigns often mass-produce content with AI tools to maintain an illusion of depth and scale.

Political parties and governments also rely on well-known social media influencers to help spread propaganda. In the aftermath of South Africa's May 2024 elections, a report from the Institute for Security Studies found that the uMkhonto weSizwe Party (MKP) had employed paid influencers to advance the unfounded narrative that the election results were "stolen" and to harass electoral commissioners. Progovernment influencers paid through an opaque network of public relations firms have been integral to shaping public opinion in the Philippines, particularly under the rule of former President Rodrigo Duterte (2016–22) and during the election to choose his successor. These influence networks sometimes persist after their patrons or clients lose office. In 2025, pro-Duterte influencers clashed with those supporting his successor, President Ferdinand "Bongbong" Marcos Jr., amid a political feud between Marcos and Vice President Sara Duterte, the former president's daughter.

> Content manipulation campaigns increasingly use technical tricks to masquerade as trusted sources, particularly by mimicking established news websites.

Some government efforts to address content manipulation have been counterproductive, ultimately damaging freedom of expression. For example, while certain laws compelled platforms to adjust their algorithms and increase transparency, others criminalized the spread of false information writ large. The latter measures have served as a pretext for illiberal and authoritarian regimes to unjustly penalize their critics. In Ethiopia, authorities have invoked the Hate Speech and Disinformation Prevention and Suppression Proclamation of 2020 to investigate and detain independent journalists in retaliation for their reporting. Kyrgyzstani officials have abused the country's 2021 Law on Protection from False Information to seek the removal of online reporting that is unfavorable to the government, such as opposition politicians' allegations that they were tortured in detention. Concurrently, governments from across the democratic spectrum have sought to delegitimize and undermine researchers and fact-checkers who seek to counter information manipulation, forcing many of them to abandon their work.

On the Horizon for Human Rights Online

Conditions for internet freedom over the next decade will be shaped in part by the ways in which governments incentivize and regulate new technologies. Three emerging developments—government-backed AI projects, the rise of satellite-based internet connectivity, and mandatory age-verification systems—will influence the near future of human rights online. But the basic challenges presented by all new technologies have remained the same over the past 15 years: how to protect rights while governing online spaces, and how to encourage innovation while establishing safeguards to prevent societal harms. The universal principles of human rights are still the best tools for navigating these straits. Freedom of expression, access to information, and privacy should guide both regulation and innovation in the years to come.

> The universal principles of human rights are still the best tools for navigating the challenges presented by new technologies.

AI sovereignty fuels digital repression

Governments around the world are pursuing ambitious agendas for AI development, and the systems developed or deployed by repressive governments could amplify existing threats to freedom of expression and privacy. As AI companies establish partnerships with governments ranging from democracies to autocracies, they will inevitably face pressure to infringe on human rights, just as telecommunications companies and social media platforms have over the past 15 years. Particularly in the world's authoritarian states, investment in AI may be misused to enable censorship and surveillance and accelerate governments' efforts to isolate their populations from the global internet.

AI tools are increasingly embedded in people's daily lives, the global economy, and government systems. Many governments' investments in AI are motivated by understandable economic and national security aims. Policymakers worldwide have declared their pursuit of "AI sovereignty," the idea that governments should retain significant control over AI systems, data, and cloud computing infrastructure, in part by keeping them within their borders or sponsoring the development of their own domestic foundational and large language models (LLMs). Despite the "sovereign" moniker and some leaders' stated concerns about US or Chinese dominance in the AI industry, many of these efforts rely on equipment or services from US- or China-based companies, which are contracted to supply cloud computing power, semiconductors, and other forms of support.

In authoritarian countries, sovereign AI initiatives could compound existing threats to free expression. Models developed under government oversight may incorporate censorship of certain content, like criticism of the authorities, or reinforce the marginalization of minority groups. Indeed, previous Freedom House research found that AI governance frameworks in China and Vietnam required generative AI chatbots to toe the Communist Party line on sensitive topics. Vietnam has seen a glut of AI investment in 2025, which a Politburo member characterized as a means of affirming the country's "historical sovereignty . . . in the digital realm." In Thailand, where criticism of the monarchy is heavily censored, the National Science and Technology Development Agency rolled out Pathumma LLM, a model trained to "understand Thai context and culture," in early 2025. While developing AI systems that reflect local culture is sensible, there is a clear risk that these initiatives will conflate local culture with state censorship.

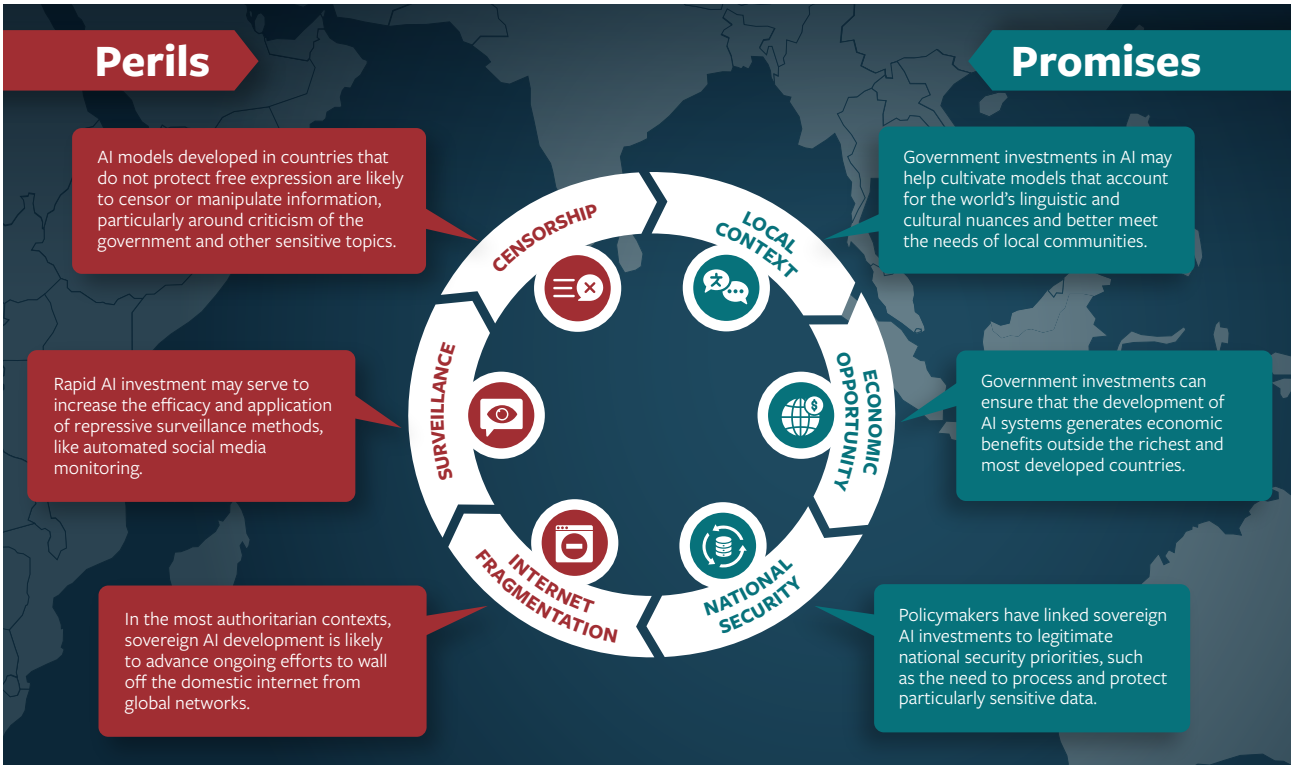
AI investments may also facilitate government surveillance, especially in authoritarian countries that lack strong privacy safeguards. The Persian Gulf monarchies have emerged as hubs for AI investment, particularly the United Arab Emirates (UAE), which announced a massive AI infrastructure project in May 2025 in partnership with the United States. The company at the forefront of the UAE's AI industry, G42, has been scrutinized by US officials for its apparent ties to Emirati and Chinese companies that specialize in surveillance and spyware technology. More broadly, the Emirati government has a long history of deploying such tools for mass monitoring and targeted surveillance of human rights defenders. In these authoritarian environments, rapid AI investment may serve to increase the efficacy and application of repressive surveillance methods.

Sovereign AI development in authoritarian contexts is likely to advance ongoing efforts to wall off the domestic internet from global networks, often referred to as "cyber sovereignty." In June 2025, the Russian and Belarusian governments launched a plan to develop AI built on "fundamental and traditional values," reflecting the same justifications that these regimes invoke when restricting access to the global internet. Russian authorities have blocked a wide array of social media platforms and messaging

> Particularly in the world's authoritarian states, investment in AI may be misused to enable censorship and surveillance and accelerate governments' efforts to isolate their populations from the global internet.

THE PERILS AND PROMISES OF AI SOVEREIGNTY

Policymakers around the world have endorsed AI sovereignty—the idea that the government should retain significant control over a country's AI systems, data, and cloud computing infrastructure. They should work with civil society to develop strong safeguards to mitigate the risk of human rights abuses and ensure that opportunities for beneficial outcomes are realized.



applications, urging users to adopt government-approved alternatives. Ahead of Belarus's sham January 2025 election, the government ordered the blocking of all websites hosted outside of the country. Iran's vice president for science announced a national AI platform in March 2025, framing it as part of a "war of chips and algorithms," and a senior scientist working on the project noted that the platform was designed to function even if Iran were to be completely disconnected from the global internet.

As democracies invest in sovereign AI capabilities in the name of economic opportunity and national security, a key test will be whether policymakers work with the private sector and civil society to establish governance frameworks that protect free expression and privacy. In July 2024, the Brazilian government announced a $4 billion investment plan for sovereign AI that would reflect the country's values; some $1 billion of the funding was allocated to state-owned technology firms. Brazilian civil society organizations have urged policymakers to embed fundamental rights safeguards as they develop the country's rules for AI governance. Indian academics and organizations have also called on authorities to put rights-respecting governance measures in place as the government moves forward with AI projects, such as research into open-source LLMs that can operate amid the country's linguistic complexity, which was announced in January 2025. AI governance measures with human rights safeguards will better position sovereign AI development to fuel innovation tailored to local needs.

Government investment in AI development reflects an understandable desire to ensure that this new wave of technology serves local interests and generates economic benefits outside the richest and most developed countries. But leaders and citizens around the world should not allow these systems to be designed or used to limit freedom of expression or violate privacy; policymakers should work alongside civil society experts to establish human rights safeguards within AI governance frameworks. The firms that provide AI infrastructure and cloud services should conduct human rights due diligence studies, particularly for projects that could impede freedom of expression or expand surveillance capabilities.

Internet freedom from low-earth orbit

A growing sector of satellite-based internet service providers is creating a dramatic shift in how people access the global network, prompting confrontations with governments that seek to control online information. Innovation in the field has lowered the cost of satellite launches, enabling a new model in which providers operate a constellation of many satellites in low-earth orbit that offer wider reach and better connection quality. These advances have brought service to areas that had yet to be reached by fiber-optic or terrestrial mobile infrastructure, or where existing access had been disrupted. However, providers are already facing pressure from authorities to carry out censorship or surveillance or to limit where services are delivered.

As the satellite internet industry expands, service providers are connecting rural communities and people in areas affected by war or natural disasters. Market leader Starlink, a subsidiary of US-based SpaceX, reported six million subscribers across 42 countries in July 2025, four years after it began offering services. Other major providers include Eutelsat OneWeb, a unit of a French firm, and Project Kuiper, owned by the US technology giant Amazon, which launched over 100 satellites in 2025. In Nigeria and Kenya, satellite providers are expanding into rural districts with little access to fixed-line or mobile broadband services, particularly as Starlink has offered low-cost connections. In Myanmar, Starlink terminals have enabled aid organizations and prodemocracy resistance groups to stay connected amid the devastating civil war, though the military regime's forces have begun seizing terminals in response.

Because they are relatively new to the market, satellite-based internet service providers have not yet widely implemented the censorship and surveillance mechanisms required by many governments, particularly those in countries ranked Not Free in *Freedom on the Net*. As a result, some authorities have sought to ban them. The Cuban government banned the entry of unregistered satellite-linked devices into the country, seizing many in March 2025. In June 2025, after the coverage period, the Iranian parliament voted to ban Starlink altogether.

A journalist in the devastated Ukrainian town of Bucha, where invading Russian forces were found to have murdered Ukrainian civilians in 2022. Satellite-based internet service providers are connecting people in areas affected by war or natural disasters. (*Photo credit: Raphael Lafargue/ABACAPRESS.COM*)

More commonly, governments have developed or enforced regulations to bring providers in line with local law, wielding the threat of bans or other penalties. These actions raise concerns about privacy and freedom of expression. The Cyberspace Administration of China, for example, issued a draft proposal in September 2024 that would require satellite internet providers to censor content in real time, maintaining the integrity of the Great Firewall even as Chinese satellite internet companies seek to compete with global peers in foreign markets. In December 2024, Kazakhstan's government threatened to ban imports of satellite communications equipment before signing an agreement to allow Starlink to enter the market in June 2025, after this report's coverage period. According to government officials, the company agreed to comply with Kazakhstan's "information and communications" laws, which have historically enabled the authorities to restrict access to the internet and surveil users. In August 2025, after the coverage period, officials in India reported that Starlink had agreed to store local users' data within the country in compliance with Indian law; the government had launched a probe into the unlawful use of the satellite service in January.

Internet connectivity in areas affected by armed conflict has been constrained by government pressure or by the risk calculations of service providers. As the two sides in Sudan's civil war destroyed the country's telecommunications infrastructure and imposed local service shutdowns, Sudanese people and aid groups turned to Starlink for emergency access to the internet. In April 2024, the company notified Sudanese users that it would limit services in the country due to regulatory constraints. Civil society organizations raised concerns about the impact of further connectivity restrictions on local humanitarian efforts, and Starlink ultimately appeared to remain accessible throughout the coverage period. Starlink has reportedly faced similar

dilemmas in Russian-occupied Ukrainian territories and Israeli-occupied Palestinian territories, which are not covered by *Freedom on the Net*.

As the satellite internet market continues to grow, providers should prepare for further government pressure to carry out censorship and hand over user data. They should use all the resources at their disposal to reject or evade any disproportionate government demands that would violate users' rights to free expression or privacy. These companies would also benefit from well-established mechanisms for multistakeholder collaboration on telecommunications services and human rights, like the Global Network Initiative, which can offer guidance on how to navigate state pressure.

The end of online anonymity

An increasing number of the world's governments are placing constraints on online anonymity. Some are limiting access to services that keep communications private. Others have mandated the use of identity verification technology as a condition for access to certain online spaces, including the most popular social media platforms. Online anonymity has long been a bulwark for free expression and access to information, empowering people to share their views online without fear of government retaliation, especially in closed societies where they could be unjustly persecuted for their political expression, their faith or nonbelief, or their identity. The restrictions on anonymity pose a direct threat to online privacy, free expression, and access to information, and could further carve up the global internet based on varying domestic rules for participation.

Though not without challenges, online anonymity has long been a bulwark for free expression and access to information, empowering people to share their views online without fear of government retaliation, especially in closed societies.

During this report's coverage period, governments from across the democratic spectrum placed limits on tools that make online privacy possible. Throughout the summer of 2024, repressive governments in Myanmar, Russia, and Venezuela blocked the encrypted messaging platform Signal, which allows its users to share and access information free from surveillance. The United Kingdom's government has sought to compel Apple to erode its end-to-end encryption standards, reportedly issuing demands to access encrypted data stored by Apple users in January 2025 and again in September 2025, after the coverage period. In February, the company limited UK-based users' access to its Advanced Data Protection feature, which allows individuals to encrypt certain forms of iCloud data. People in 17 of the 72 countries covered by *Freedom on the Net* experienced blocks on end-to-end encrypted communications platforms between January 2020 and March 2025, according to recent Freedom House research published in partnership with the European University Institute.

Laws requiring identity verification to post online content present another avenue for undermining anonymity, and they have occasionally been enacted by authoritarian governments to curtail dissent. In Vietnam, a December 2024 law required users of social media platforms to authenticate their accounts with their government-issued identification documents or their Vietnamese mobile phone numbers, which are themselves subject to real-name registration. Real-name registration has been required to access internet services in China since at least 2012, and during the coverage period regulators experimented with a system that would centralize age-verification services for social media platforms through a government-controlled digital identity system. Belarusians posting content to local websites have been required to register their identities since 2019. These rules present a serious risk of harm, as people in all three countries—and many others—routinely face arrest and heavy criminal penalties for dissent expressed online.

Similar requirements in democracies are ushering in a new paradigm for access to information and online communication, as policymakers impose age-verification laws in the name of online safety and child protection. These laws may oblige users seeking certain content to upload a government identification card or submit to "age assurance" technology that employs facial analysis to estimate a person's age. In November 2024, the Australian government passed a law that would ban children under 16 from accessing social media platforms,

A CRISIS FOR ONLINE ANONYMITY

An increasing number of the world's governments are placing constraints on online anonymity, undermining an essential bulwark for free expression and creating new privacy risks.

the most expansive measure of its kind; it is set to enter into force in December 2025. A March 2025 Indonesian regulation requires online platforms to implement age-verification features and enforce age restrictions based on whether they host pornographic or violent content, offer material with a potential for psychological harm, or have other "high-risk" features.

In some cases, these laws have led platforms to impose invasive age-verification measures for all their users, or to pull out of the market in question due to compliance burdens. Age-verification features of the United Kingdom's Online Safety Act entered into force in July 2025, requiring users to provide government identification documents, facial scans, or credit cards to prove that they are not children; the rules apply to websites with broadly defined "harmful content," leaving the websites themselves responsible for determining which content meets the definition. As they rolled out these features, there were notable examples of overbroad application, including for forums on LGBT+ issues, journalism, and public health. In the United States, a Mississippi state law that entered into force in August 2025, after the coverage period, required platforms to deploy age-verification systems to prevent children from creating accounts without parental consent. Several small platforms, like the social media application Bluesky and the blogging service Dreamwidth, have blocked access in Mississippi because of the compliance burden.

Other measures focus on pornography and sexual content. In the United States, a June 2025 Supreme Court decision affirmed that Texas could require age-verification features for "sexually explicit material," finding that the state's law "only incidentally burdens the protected speech of adults." At least 24 US states had passed age-verification laws focused on such content by the end of the coverage period.

While protecting children online is an important and legitimate policy aim, measures that compel platforms to verify people's identities introduce a range of new risks. In countries with weak rule of law and widespread government

surveillance, age-verification laws are ripe for abuse. Even in countries with strong privacy laws in place, cybersecurity breaches at companies that carry out age verification or provide third-party tools could result in the leak of people's identity documents or biometric data. The danger is more than hypothetical. In the 16 years since the launch and widespread adoption of India's Aadhaar biometric identification system, breaches of third-party databases have resulted in leaks of hundreds of millions of Aadhaar numbers, fueling a black market for perpetrators of fraud and cybercrime. These companies are also a target for state-backed hackers. In August 2025, it was reported that a yearslong operation—dubbed Salt Typhoon—to infiltrate US telecommunications infrastructure had enabled a group of Chinese government-linked hackers to exfiltrate data pertaining to hundreds of millions of Americans.

Other measures are more effective at bridging child protection and fundamental rights. These include tailored regulation to require stronger default privacy settings for children on platforms that allow minors to create accounts, more stringent data protection standards for young people, and adequate resources for investigations into online child abuse. Platforms that allow children to create accounts also have an obligation to ensure that their services offer strong privacy and security safeguards by design. Meanwhile, promising efforts to develop privacy-preserving and rights-respecting methods for age verification are underway, and technologists, innovation-minded governments, and civil society groups should work together to encourage support and adoption.

By embedding safeguards for free expression and privacy into new technologies at the earliest stage of development, democratic societies can ensure that they will fuel improvements for global internet freedom.

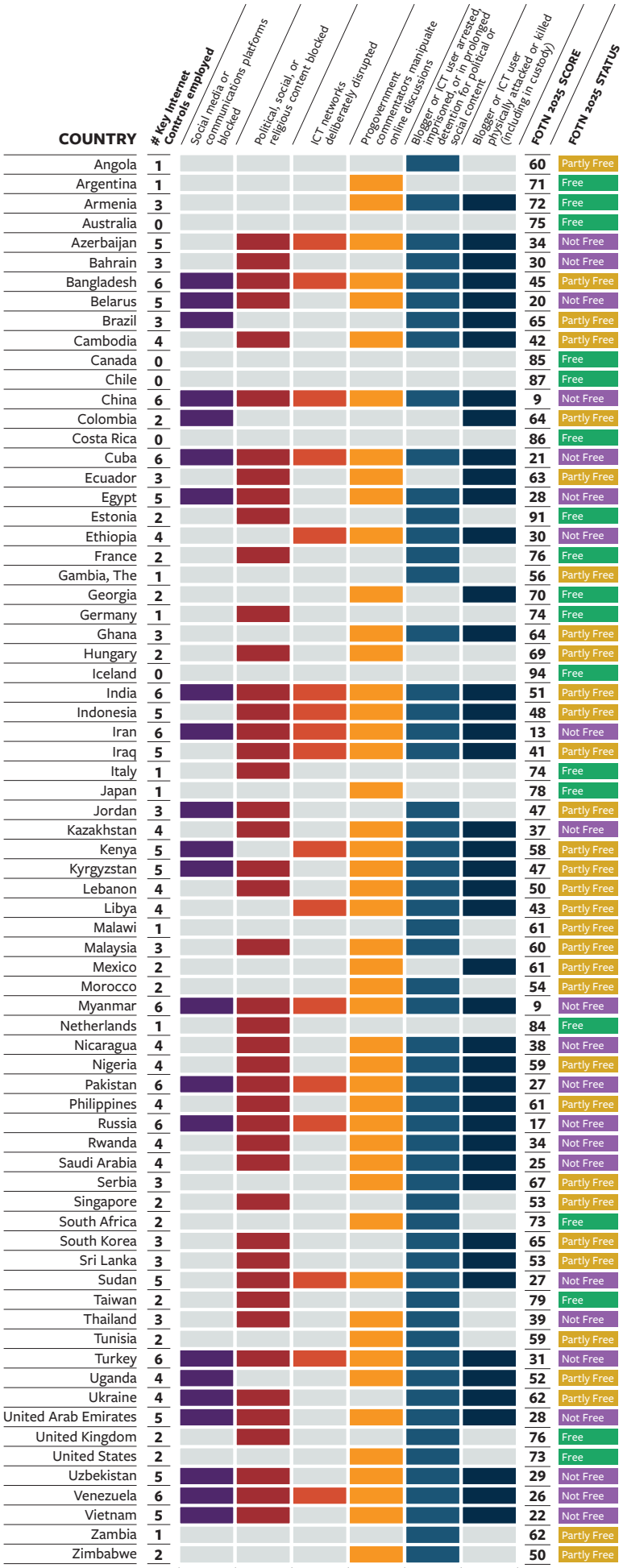
Acting now for a freer future

Fifteen years of *Freedom on the Net* analysis has shown that innovation presents both opportunities for and challenges to human rights online. Social media platforms, initially heralded as drivers of political and economic liberation, have been exploited by autocratic regimes and other unscrupulous political forces to spew propaganda, censor protected expression, and surveil dissidents. The next wave of new technologies will transform how people exercise their rights in digital spaces.

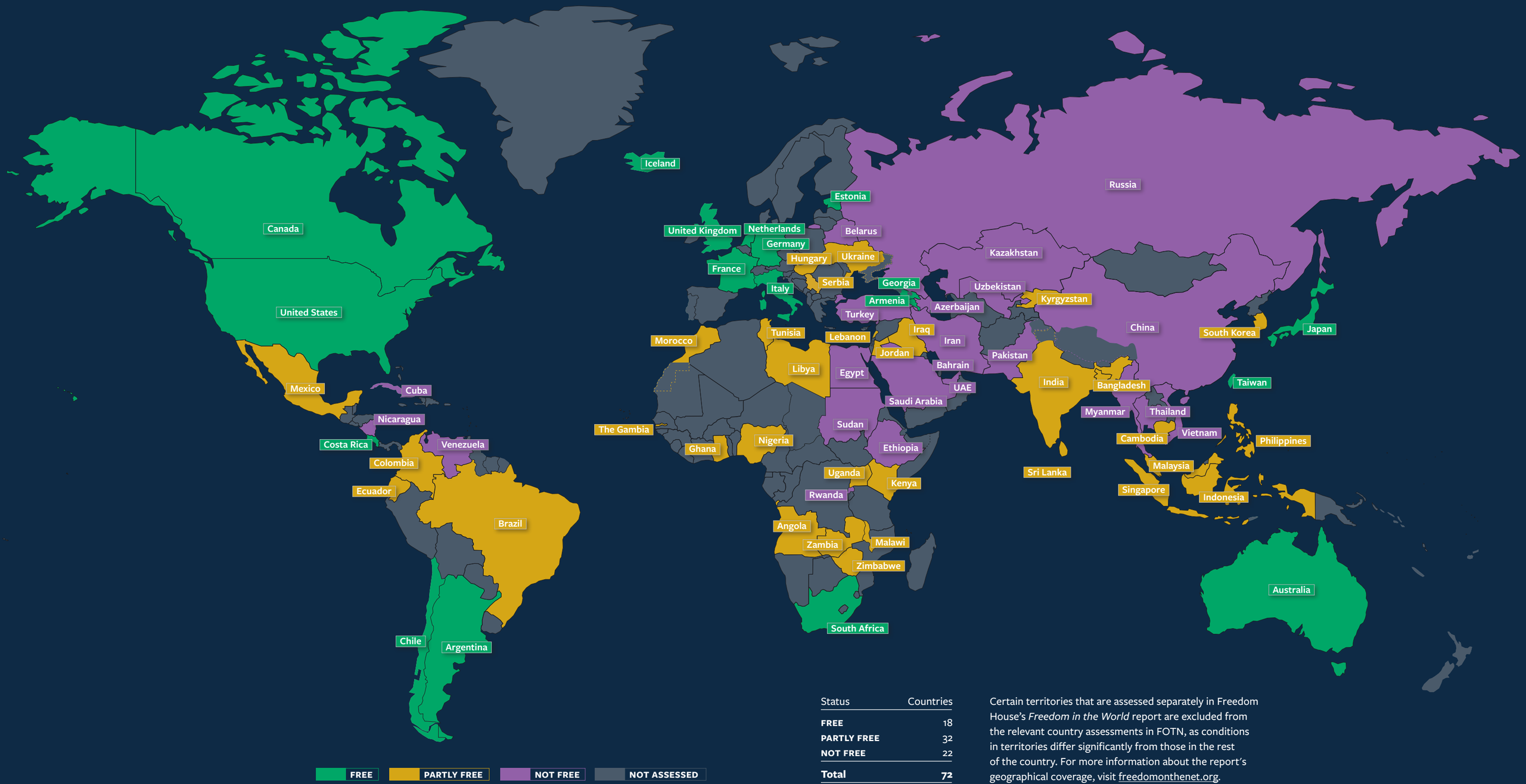
AI is already becoming integrated into our daily lives, satellite internet service is expanding connectivity and competing with incumbent providers, and identity verification technology is reshaping access to online content and communities. By embedding safeguards for free expression and privacy into these systems at the earliest possible stage of development, democratic societies can ensure that they will fuel improvements for global internet freedom rather than contributing to another period of decline.

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 2024 to May 2025. The Key Internet Controls reflect restrictions on content of political, social, or religious nature. Freedom House reduced the number of Key Internet Controls tracked in the 2025 edition because of budget constraints.



FREEDOM ON THE NET 2025

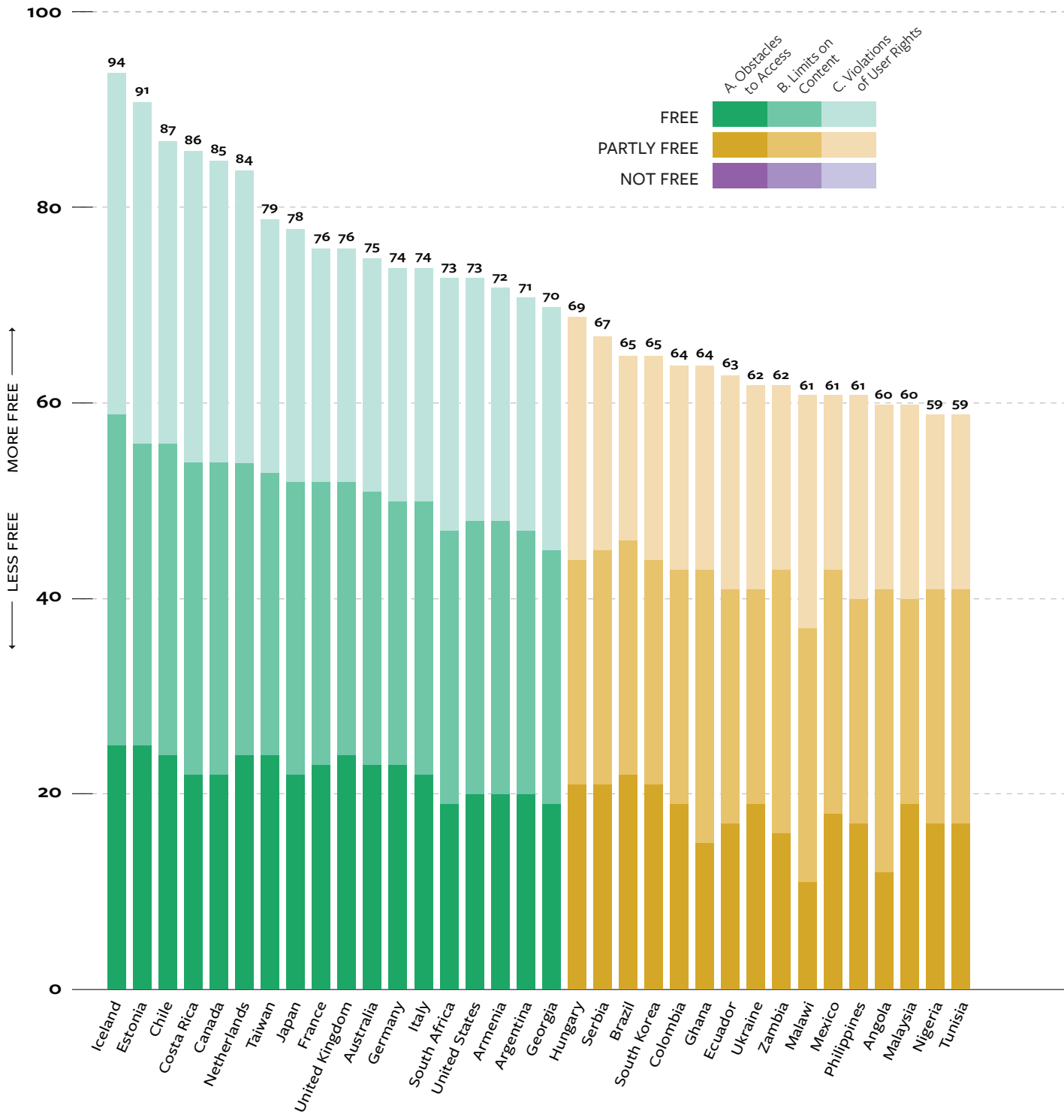


Status	Countries
FREE	18
PARTLY FREE	32
NOT FREE	22
Total	**72**

Certain territories that are assessed separately in Freedom House's *Freedom in the World* report are excluded from the relevant country assessments in FOTN, as conditions in territories differ significantly from those in the rest of the country. For more information about the report's geographical coverage, visit freedomonthenet.org.

GLOBAL RANKINGS

100 = Most Free 0 = Least Free



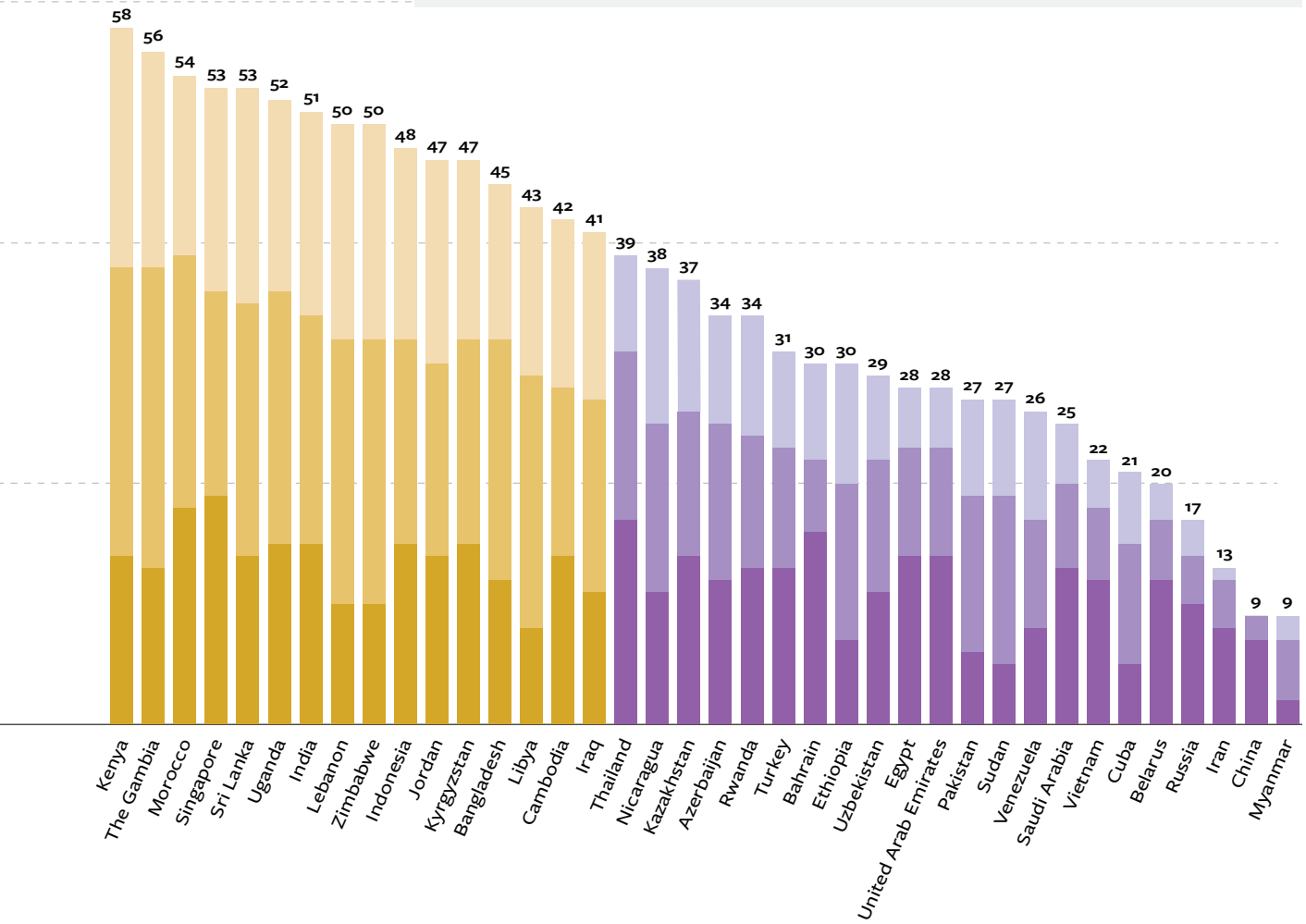
Freedom on the Net 2025 covers 72 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems. Each country receives a numerical score from **100 (the most free)** to **0 (the least free)**, which serves 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.



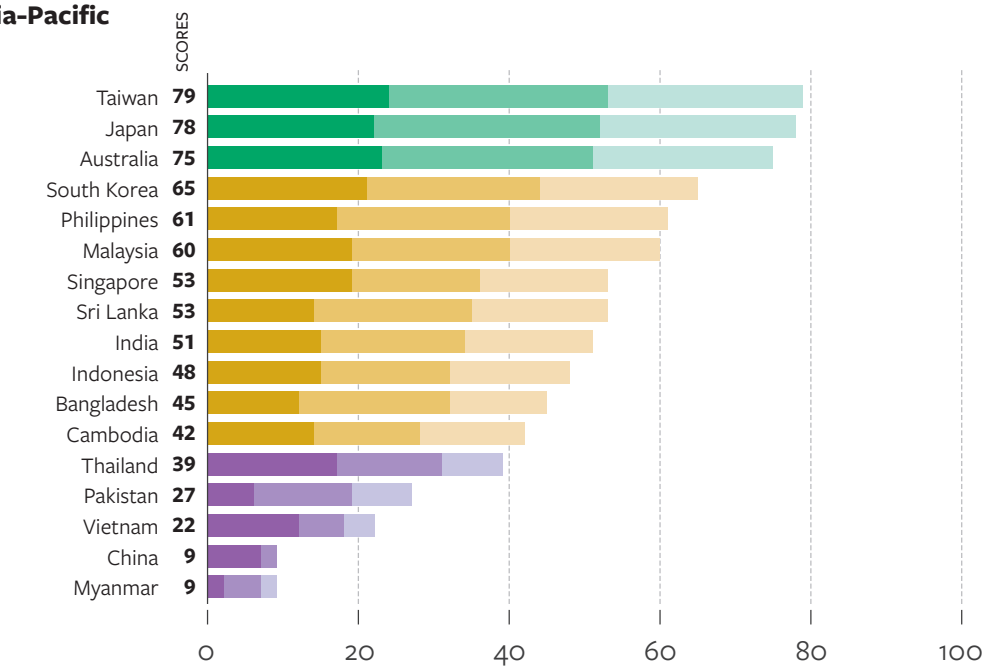
REGIONAL RANKINGS

Freedom on the Net 2025 covers 72 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

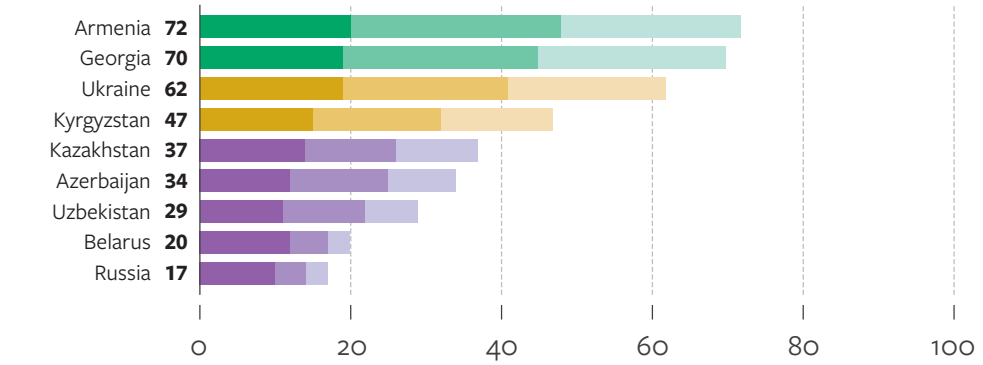
A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights

0 = Least Free
100 = Most Free

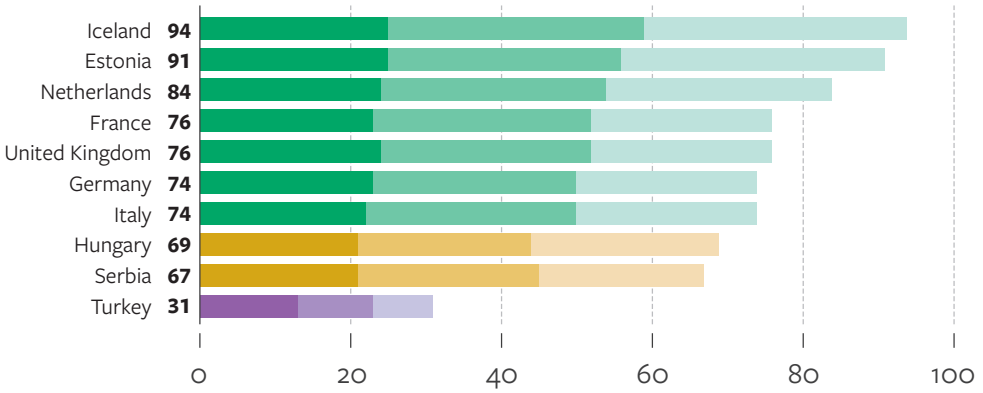
Asia-Pacific



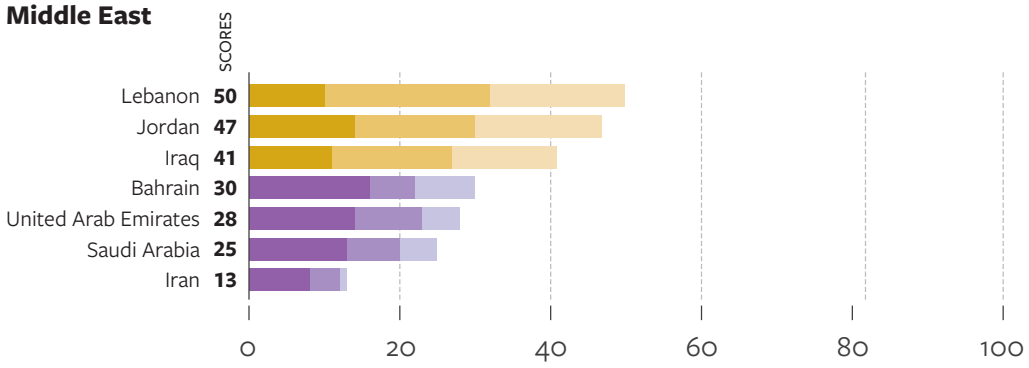
Eurasia



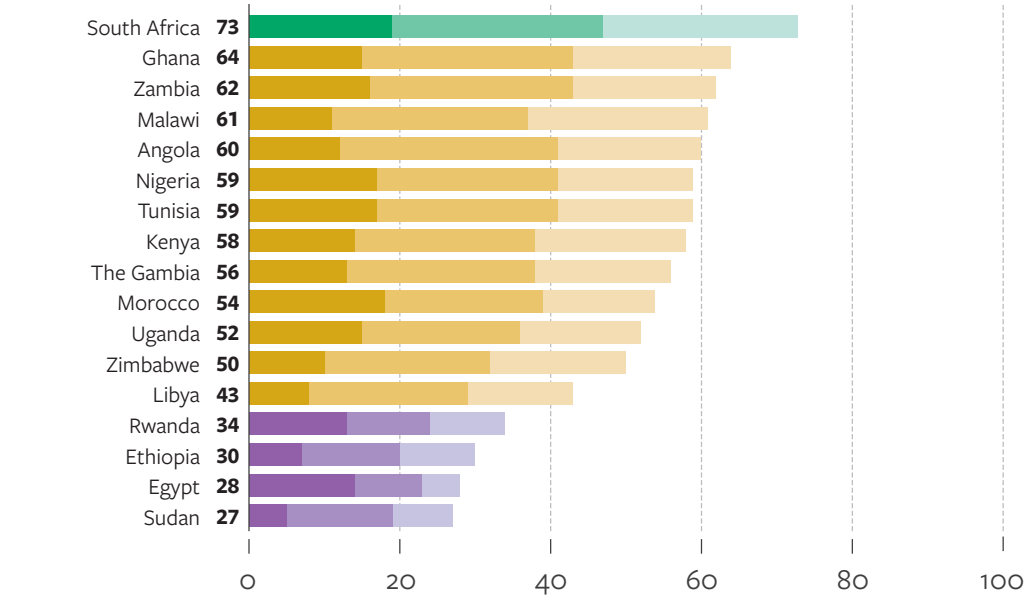
Europe



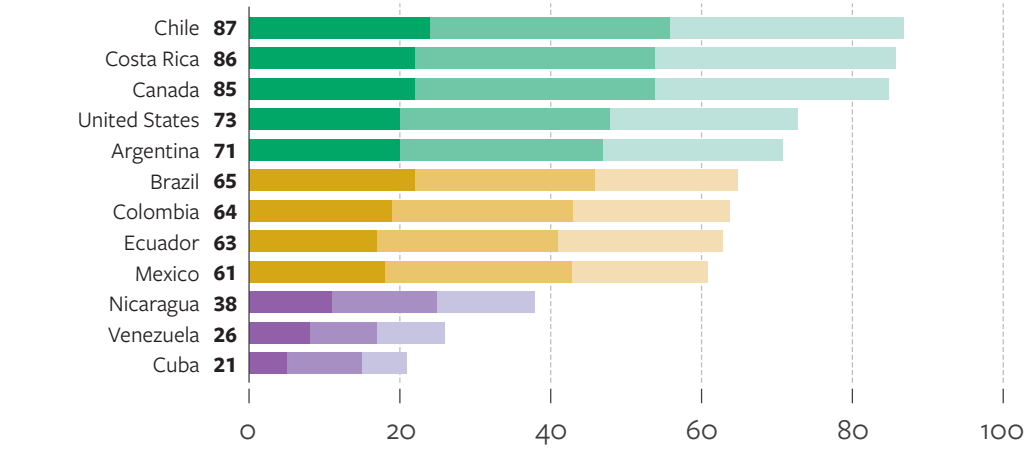
Middle East



Africa



Americas



Policy Recommendations

Policymakers, the tech industry, and civil society should work together to address the global decline in internet freedom.

Over the 15 consecutive years of internet freedom's decline, Freedom House and other members of the digital rights community have offered clear, practical recommendations for protecting freedom online and reversing this trajectory. However, implementation has lagged behind rhetoric and the velocity of change in digital infrastructure and tools. As democracies cut foreign assistance budgets and private companies retreat from rights-respecting approaches, the global balance of digital power may tip further toward those who see the internet as a tool of control rather than of freedom. The urgency to act has never been greater. Protecting human rights online and rebuilding a free, open, and secure internet will require sustained commitment, resources, collaboration, and imagination from governments, the private sector, and civil society.

Civil society actors are indispensable partners in defending human rights online and countering authoritarian digital repression. To ensure that civil society can continue to build tools that advance rights, provide essential analysis, and conduct critical advocacy and programming, democratic governments and companies must strengthen—not reduce—their financial and political support. There is no time to waste: with coordinated action, it is still possible to reclaim the internet as a space for freedom, accountability, and human dignity.

15 Consecutive Years of Decline: Addressing Key Drivers of Digital Repression

Freedom on the Net research over the past 15 years has illustrated how the major drivers of digital repression are consistently related to **restrictions on free expression, the manipulation of the online environment**, and **restrictions on privacy and disproportionate government surveillance**. The following recommendations outline how governments and companies can and should address these perennial challenges. Many of these recommendations will look familiar—because they are. The fundamentals of protecting human rights online have not changed, and sustained implementation of these principles remains essential to reversing and preventing global declines in internet freedom.

1. COUNTERING RESTRICTIONS ON FREEDOM OF EXPRESSION

Freedom of expression online has been and is increasingly under attack as governments shut off internet connectivity, block social media platforms, and restrict access to websites that host political, social, and religious speech. Protecting freedom of expression will require strong legal and regulatory safeguards for digital communications.

Governments

Governments should maintain access to internet services, digital platforms, and anticensorship technology, particularly during elections, protests, and periods of unrest or conflict. Imposing outright or arbitrary bans on social media and messaging platforms unduly restricts free expression. Governments should address any legitimate risks posed by these platforms through existing democratic mechanisms, such as regulatory action, security audits, parliamentary scrutiny, and legislation passed in consultation with civil society. Other methods to address legitimate security problems include strengthening legal requirements for platform transparency, data privacy, cybersecurity, and responsibility for mandatory human rights due diligence and risk assessments. Any legal restrictions for online content should adhere to international human rights standards of legality, necessity, and proportionality, and include robust oversight, transparency, and consultation with civil society and the private sector.

Legal frameworks addressing online content should uphold internationally recognized human rights and establish special obligations for companies that are tailored to their size and services, incentivize platforms to improve their own standards, and

require human rights due diligence and reporting. Such obligations should prioritize transparency across core products and practices, including content moderation, recommendation and algorithmic systems, collection and use of data, and political and targeted advertising. Laws should ensure that vetted researchers are able to access platform data in a privacy-protecting way, allowing them to provide insights for policy development and civil society's broader analysis and advocacy efforts.

Safe-harbor protections for intermediaries should remain in place for most of the user-generated and third-party content appearing on platforms, so as not to encourage these companies to impose excessive restrictions that inhibit free expression. Laws should also reserve final decisions on the legality and removal of content for the judiciary. Independent regulators with sufficient resources and expertise should be empowered to oversee the implementation of laws, conduct audits, and ensure compliance.

Companies

Companies should commit to respecting the rights of people who use their platforms or services, and to addressing any adverse impact that their products might have on human rights. Companies should support the accessibility of anticensorship technologies, including by making them more affordable, and resist government orders to shut down internet connectivity or ban digital services. Service providers should use all available legal channels to challenge content removal requests—whether official or informal—that would violate international human rights standards, particularly when they relate to the accounts of human rights defenders, civil society activists, journalists, or other at-risk individuals.

If companies cannot resist such demands in full, they should ensure that any restrictions or disruptions are as limited as possible in duration, geographic scope, and type of content affected. Companies should thoroughly document government demands internally and notify people who use their platforms as to why connectivity or content may be restricted, especially in countries where government actions lack transparency. When faced with a choice between a ban of their services and complying with censorship orders, companies should bring strategic legal cases that challenge government overreach, in consultation or partnership with civil society.

2. COUNTERING MANIPULATION OF THE ONLINE ENVIRONMENT

The potential consequences of false, misleading, and incendiary content are especially grave during election periods, underscoring the need to protect access to reliable information. Efforts to address the problem should start well before campaigning begins and continue long after the last vote is cast. Great care should be given to ensure that efforts to address information manipulation also prioritize the protection of free speech

Governments

Governments should encourage a whole-of-society approach to fostering a high-quality, diverse, and trustworthy information space. The Global Declaration on Information Integrity Online identifies best practices for safeguarding the information ecosystem, to which governments should adhere. For example, the declaration lays out recommendations for how to support an information ecosystem that "respects human rights and supports open, safe, secure, prosperous and democratic societies," enables the production of "accurate, trustworthy, and reliable information," and protect populations that are often targeted for online harassment and threats.

Laws aimed at increasing platform responsibility as described above—such as those that boost transparency, provide platform data to vetted researchers, and safeguard free expression—are pivotal to countering threats to a reliable information ecosystem. Governments should also support independent online media and empower ordinary people with the tools they need to identify false or misleading information and to navigate complex media environments. They should proactively and directly engage with their constituencies to disseminate credible information and build trust. Governments should support the work of independent civil society organizations that conduct fact-checking efforts, civic education initiatives, and digital literacy training, as well as those that focus on human rights and democracy work more broadly.

Companies

The private sector has a responsibility to ensure that its products contribute to, and do not undermine, a diverse and reliable information space and the protection of freedom of expression. Companies should invest in staff tasked with work related to public policy, access to reliable information, trust and safety, and human rights, including teams of regional and country specialists. These teams should collaborate closely with civil society groups around the world to understand the local impact of their companies' products and policies. Without such expertise, the private sector is ill-equipped to address harassment, abuse, and false and misleading information that can have serious offline consequences. Social media firms should also develop mechanisms for and expand researchers' access to platform data, allowing for independent analysis of harassment, influence operations, and other trends online.

PROTECTING DIGITAL RIGHTS IN THE FUTURE

Even as the main drivers of repression remain unchanged, new forces are beginning to redefine the contours of digital freedom: **government-backed AI development, the growth of satellite internet, and the proliferation of age-verification mandates**. Freedom House and its partners are monitoring these developments, as their governance and implementation could profoundly affect the future of human rights online.

Government-backed AI development: As governments deploy AI services and develop their own systems, they should conduct human rights impact assessments to ensure that their products do not curtail freedom of expression and other fundamental rights. This includes identifying key human rights risks, empowering impacted communities to comment on potential human rights impacts, developing and implementing mitigation plans, and evaluating the success or shortcomings of those plans. In addition, governments should limit data collection for AI systems to strictly what is needed to provide a necessary service. It is also important that governments transparently communicate with stakeholders about how they are addressing actual and potential human rights impacts. Similarly, when the private sector partners with governments to develop AI systems for public services, they should conduct human rights due diligence. Localization and customization should never be prioritized over human rights principles.

The growth of satellite internet: Satellite internet providers should use all resources at their disposal to reject or contest disproportionate government demands that contravene international human rights standards or lack a valid judicial warrant. The Global Network Initiative, as a multistakeholder forum dedicated to government and company policies and practices relating to technology and human rights, offers guidance around navigating and mitigating these pressures.

The proliferation of age-verification mandates: Governments should avoid mandating that platforms implement age-verification or age-assurance systems, which often harm privacy and security. If such measures are put in place, they should embed data-minimization requirements, limit the provision of data to third parties and government agencies, and require the strongest possible cybersecurity measures. Governments should create stronger privacy protections for children, such as by requiring platforms that allow children to create accounts to make them private by default, and to alter algorithmic recommendation systems to limit children's exposure to harmful content. They should also provide greater resources for investigations into online child abuse. Platforms that allow children to create accounts have an obligation to ensure that their services offer controls to ensure strong privacy and security safeguards, and should consult widely with civil society about how to protect children without infringing on their rights.

Companies should continue to develop effective methods to watermark AI-generated content, which entails the use of a cryptographic signature. While not a silver-bullet solution, watermarking could be useful when combined with other labeling of AI-generated media for individual awareness, as well as coordination with civil society, academia, and technical experts on industry standards for documenting the provenance of specific content. When assessing how to appropriately enhance content provenance, companies should consider privacy risks for human rights defenders and other vulnerable users.

As more government agencies seek to engage with technology firms, companies should tailor their engagement based on an assessment of whether the bodies operate independently and without political interference, in consultation with in-country civil society. Companies should specifically adopt processes to ensure that engagement does not undermine free expression, access to information, due process, and other fundamental rights. For example, formal and informal demands for content removal should be thoroughly documented and evaluated for human rights impact.

3. COUNTERING RESTRICTIONS ON PRIVACY AND DISPROPORTIONATE GOVERNMENT SURVEILLANCE

Comprehensive data-protection regulations and industry policies on data protection are essential for upholding privacy and combating disproportionate government surveillance, but they require careful crafting to ensure that they do not contribute to internet fragmentation—the siloing of the global internet into nation-based segments—and cannot be used by governments to undermine privacy and other fundamental freedoms

Governments

Democracies should collaborate to create interoperable privacy regimes that comprehensively safeguard user information, while also allowing data to flow across borders to and from jurisdictions with similar levels of protection. Individuals should be given control over their information, including the right to access it, delete it, and easily transfer it to providers of their choosing. Laws should include guardrails that limit the ways private companies can use personal data for AI development and in their AI systems, including algorithmic recommendations.

Governments should ensure that independent regulators and oversight mechanisms have the ability, resources, and expertise to ensure foreign and domestic companies' compliance with updated privacy, nondiscrimination, and consumer-protection laws.

Government surveillance programs should adhere to the International Principles on the Application of Human Rights to Communications Surveillance, a framework agreed upon by a broad consortium of civil society groups, industry leaders, and scholars, and launched at the UN Human Rights Council in Geneva in September 2013 by the Electronic Frontier Foundation. The principles, which state that all communications surveillance must be legal, necessary, and proportionate, should also be applied to AI-driven and biometric surveillance technologies, targeted surveillance tools like commercial spyware and extraction software, and open-source intelligence methods such as social media monitoring.

Companies

Companies should mainstream end-to-end encryption in their products, support anonymity software, and uphold other robust security protocols, including by notifying victims of surveillance abuses and resisting government requests to provide special decryption access. Digital platforms should use all available legal channels to challenge problematic requests from state agencies, whether they are official or informal, especially when they relate to the accounts of human rights defenders, civil society activists, journalists, or other at-risk individuals.

Companies should minimize the collection of personal information, such as health, biometric, and location data, and limit how third parties can access and use it. Companies should also clearly explain to people who use their services what data are being collected and for what purpose

What We Measure

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

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

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

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

THE RESEARCH AND SCORING PROCESS

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

A. **Obstacles to Access** details infrastructural, economic, and political barriers to access; government decisions to shut off connectivity or block specific applications or technologies; legal, regulatory, and ownership control over internet service providers; and the independence of regulatory bodies.

B. **Limits on Content** analyzes legal regulations on content; technical filtering and blocking of websites; other forms of censorship and self-censorship; the vibrancy and diversity of online information space; and the use of digital tools for civic mobilization.

C. **Violations of User Rights** tackles legal protections and restrictions on free expression; surveillance and privacy; and legal and extralegal repercussions for online speech and activities, such as imprisonment, cyberattacks, or extralegal harassment and physical violence.

Each question is scored on a varying range of points. The subquestions guide researchers regarding factors they should consider while evaluating and assigning points, though not all will be relevant to every country. Under each question, a higher number of points is allotted for a freer situation, while a lower number of points is allotted for a less free environment. Points add up to produce a score for each of the categories, and a country's total points for all three categories represent its final score (0–100). Based on the score, Freedom House assigns the following internet freedom statuses:

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

Freedom House adopted a modified report production process for *Freedom on the Net 2025* because of budget constraints. Staff members conducted robust research to analyze developments in the 72 countries covered by the report. Staff also reviewed each country's scores based on established coding guidelines, through careful consideration of events, laws, and practices relevant to each indicator, and consulted independent experts to assess the comparative reliability and integrity of the scores for a majority of countries. Following the scoring process, Freedom House staff produced summaries of key developments in each country, and again consulted with independent experts on the summaries for a subset of countries. Staff members conducted additional qualitative analysis on every country to identify the year's most important global findings and emerging trends.

In previous editions, Freedom House staff invited at least one researcher or organization to serve as the author for a full narrative report on each country, training them to assess internet freedom developments according to the project's comprehensive research methodology. These authors submitted draft scores and country reports and attended a ratings review meeting focused on their region. During the meetings, participants reviewed, critiqued, and adjusted the draft scores based on the established coding guidelines. After completing the regional and country consultations, Freedom House staff edited all country reports and performed a final review of all scores to ensure their comparative reliability and integrity.

Freedom on the Net scores were inverted in the 2019 edition to align with the scoring system for *Freedom in the World*, Freedom House's flagship report on political rights and civil liberties.

Checklist of Questions

A. OBSTACLES TO ACCESS

(*0–25 POINTS*)

1. **Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?** (*0–6 points*)
   - Do individuals have access to high-speed internet services at their home, place of work, libraries, schools, and other venues, as well as on mobile devices?
   - Does poor infrastructure (including unreliable electricity) or catastrophic damage to infrastructure (caused by events such as natural disasters or armed conflicts) limit residents' ability to access the internet?

2. **Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?** (*0–3 points*)
   - Do financial constraints—such as high prices for internet services, excessive taxes imposed on such services, or state manipulation of the relevant markets—make internet access prohibitively expensive for large segments of the population?
   - Are there significant differences in internet penetration and access based on geographical area, or for certain ethnic, religious, gender, LGBT+, migrant, and other relevant groups?
   - Do pricing practices by service providers and digital platforms contribute to a digital divide in terms of what types of content individuals with different financial means can access?

3. **Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?** (*0–6 points*)
    - Does the government (or the de-facto government in a given area) restrict, or compel service providers to restrict, internet connectivity by slowing or shutting down internet connections during specific events (such as protests or elections), either locally or nationally?
    - Does the government centralize internet infrastructure in a manner that could facilitate restrictions on connectivity?
    - Does the government block, or compel service providers to block, social media platforms and communication apps that serve in practice as major conduits for online information?
    - Does the government block, or compel service providers to block, certain protocols, ports, and functionalities within such platforms and apps (e.g., Voice-over-Internet-Protocol or VoIP, video streaming, multimedia messaging, Secure Sockets Layer or SSL), either permanently or during specific events?
    - Do restrictions on connectivity disproportionately affect marginalized communities, such as inhabitants of certain regions or those belonging to different ethnic, religious, gender, LGBT+, migrant, diaspora, and other relevant groups?

4. **Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?** (*0–6 points*)
    - Is there a legal or de facto monopoly on the provision of fixed-line, mobile, and public internet access?
    - Does the state place extensive legal, regulatory, or economic requirements on the establishment or operation of service providers?
    - Do operational requirements, such as retaining customer data or preventing access to certain content, place an onerous financial burden on service providers?

5. **Do national regulatory bodies that oversee service providers, digital platforms, and the internet more broadly fail to operate in a free, fair, and independent manner?** (*0–4 points*)
    - Are there explicit legal guarantees that protect the independence and autonomy of regulatory bodies overseeing the internet (exclusively or as part of a broader mandate) from political or commercial interference?
    - Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' legitimate interests?
    - Are decisions taken by regulatory bodies relating to the internet fair and to take meaningful notice of comments from stakeholders in society?
    - Are decisions taken by regulatory bodies apolitical and independent from changes in government?
    - Do decisions taken by regulatory bodies protect internet freedom, including by ensuring service providers, digital platforms, and other content hosts behave fairly?

B. LIMITS ON CONTENT

(*0–35 POINTS*)

1. **Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?** (*0–6 points*)
    - Does the state use, or compel service providers to use, technical means to restrict freedom of opinion and expression, for example by blocking or filtering websites and online content featuring journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression?
    - Does the state use, or compel service providers to use, technical means to block or filter access to websites that may be socially or legally problematic (e.g., those related to gambling, pornography, copyright violations, illegal drugs) in lieu of more effective remedies, or in a manner that inflicts collateral damage on content and activities that are protected under international human rights standards?
    - Does the state block or order the blocking of entire social media platforms, communication apps, blog-hosting platforms, discussion forums, and other web domains for the purpose of censoring the content that appears on them?

- Is there blocking of tools that enable individuals to bypass censorship, such as virtual private networks (VPNs)?
- Does the state procure, or compel services providers to procure, advanced technology to automate censorship or increase its scope?

2. **Do state or nonstate actors employ legal, administrative, or other means to force publishers, digital platforms, content hosts, or other intermediaries to delete content, particularly material that is protected by international human rights standards?** (*0–4 points*)
   - Are administrative, judicial, or extralegal measures used to order the deletion of content from the internet, particularly journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression, either prior to or after its publication?
   - Do publishers, digital platforms, content hosts (including intermediaries such as app stores and content delivery networks) arbitrarily remove such content due to informal or formal pressure from government officials or other powerful political actors?
   - Do publishers, digital platforms, content hosts, and other intermediaries face excessive or improper legal responsibility for opinions expressed by third parties transmitted via the technology they supply (i.e., intermediary liability), incentivizing them to remove such content?

3. **Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?** (*0–4 points*)
   - Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content abide by international human rights standards and are proportional to their stated aim?
   - Do specific laws or binding legal decisions require publishers, digital platforms, ISPs, content hosts, generative artificial intelligence systems, and other intermediaries to restrict access to online material, particularly that which is protected under international human rights standards?
   - Are those that restrict content—including state authorities, ISPs, content hosts, digital platforms, and other intermediaries—transparent about what content is blocked, deleted, or otherwise limited, including to the public and directly to the impacted user?
   - Are rules for the restriction of content clearly defined, openly available for individuals to view, and implemented in a consistent and nondiscriminatory manner?
   - Do individuals whose content is subjected to censorship have access to efficient and timely avenues of appeal with the actor responsible for restricting that content, or with independent oversight bodies, including mechanisms set up by the state or industry?

4. **Do journalists, commentators, and ordinary people practice self-censorship online?** (*0–4 points*)
   - Do internet users in the country engage in self-censorship on important political, social, or religious issues, including on public forums and in private communications?
   - Does fear of retribution, censorship, state surveillance, or data collection practices have a chilling effect on online speech or cause individuals to avoid certain online activities of a civic nature?
   - Where widespread self-censorship online exists, do some journalists, commentators, or ordinary individuals continue to test the boundaries, despite the potential repercussions?

5. **Are online sources of information controlled or manipulated by the government or other powerful actors to advance a favored interest?** (*0–4 points*)
   - Do political leaders, government agencies, political parties, or other powerful actors directly manipulate information or disseminate false or misleading information via state-owned news outlets, official social media accounts/groups, or other formal channels?
   - Do government officials or other actors surreptitiously employ or encourage individuals, companies, or automated systems to generate or artificially amplify favored narratives or smear campaigns on social media?

- Do government officials or other powerful actors pressure or coerce online news outlets, journalists, or other online commentators to follow a particular editorial direction in their reporting and commentary?
- Do authorities issue official guidelines or directives on coverage to online media outlets, including instructions to downplay or amplify certain comments or topics?
- Do government officials or other actors bribe or use close economic ties with online journalists, commentators, or website owners in order to influence the content they produce or host?
- Do campaigns coordinated by foreign or domestic actors to spread false or misleading information for political purposes have a significant impact on public debate?

6. **Are there economic, regulatory, or other constraints that negatively affect individuals' ability to publish content online?** (*0–3 points*)
   - Are favorable informal connections with government officials or other powerful actors necessary for online media outlets, content hosts, or digital platforms (e.g., search engines, email applications, blog-hosting platforms) to be economically viable?
   - Does the state limit the ability of online media or other content hosts to accept advertising or investment, particularly from foreign sources, or does it discourage advertisers from conducting business with disfavored online media or other content hosts?
   - Do onerous taxes, regulations, or licensing fees present an obstacle to participation in, establishment of, or management of digital platforms, news outlets, blogs, or social media groups/channels?
   - Do ISPs manage network traffic and bandwidth availability in a manner that is transparent, is evenly applied, and does not discriminate against users or producers of content based on the nature or source of the content itself (i.e., do they respect "net neutrality" with regard to content)?

7. **Does the online information landscape lack diversity and reliability?** (*0–4 points*)
   - Are people able to access a range of local, regional, and international news sources that convey independent, balanced views in the main languages spoken in the country?
   - Do online media outlets, social media pages, blogs, and websites represent diverse interests, experiences, and languages within society, for example by providing content produced by different ethnic, religious, gender, LGBT+, migrant, diaspora, and other relevant groups?
   - Does a lack of competition among digital platforms, content hosts, and other intermediaries undermine the diversity of information to which people have access?
   - Does the presence of false or misleading content undermine users' ability to access independent, credible, and diverse sources of information?
   - Does false or misleading content online significantly contribute to offline harms, such as harassment, property destruction, physical violence, or death?
   - If there is extensive censorship, do users employ VPNs and other circumvention tools to access a broader array of information sources?

8. **Do conditions impede individuals' ability to form communities, mobilize, and campaign online, particularly on political and social issues?** (*0–6 points*)
   - Can people freely participate in civic life online and join online communities based around their political, social, or cultural identities without fear of retribution or harm?
   - Do civil society organizations, activists, and communities organize online on political, social, cultural, and economic issues, including during electoral campaigns and nonviolent protests, and without fear of retribution or harm?
     Do state or other actors limit access to online tools and websites (e.g., social media platforms, messaging groups, petition websites) for the purpose of restricting free assembly and association online?
   - Does the state use legal or other means (e.g. criminal provisions, detentions, surveillance) to restrict free assembly and association online?

C. VIOLATIONS OF USER RIGHTS

(0–40 POINTS)

1. **Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?** (*0–6 points*)
    - Does the constitution contain language that provides for freedom of expression, access to information, and press freedom generally?
    - Are there laws or binding legal decisions that specifically protect online modes of expression, access to information, and press freedom?
    - Do executive, legislative, and other governmental authorities comply with these legal decisions, and are these decisions effectively enforced?
    - Is the judiciary independent, and do senior judicial bodies and officials support free expression, access to information, and press freedom online?

2. **Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?** (*0–4 points*)
    - Do specific laws—including penal codes and those related to the media, defamation, cybercrime, cybersecurity, and terrorism—criminalize online expression and activities that are protected under international human rights standards (e.g., journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression)?
    - Are restrictions on online activities defined by law, narrowly circumscribed, and both necessary and proportionate to address a legitimate aim?

3. **Are individuals penalized for online activities, particularly those that are protected under international human rights standards?** (*0–6 points*)
    - Are writers, commentators, journalists, bloggers, or social media users subject to civil liability, imprisonment, arbitrary detention, police raids, the stripping of citizenship, or other legal sanction for publishing, sharing, or accessing material on the internet in contravention of international human rights standards?
    - Are penalties for defamation; spreading false information or "fake news"; cybersecurity, national security, terrorism, and extremism; blasphemy; insulting state institutions and officials; or harming foreign relations applied unnecessarily and disproportionately?

4. **Does the government place restrictions on anonymous online communication or encryption?** (*0–4 points*)
    - Are website owners, bloggers, or users in general required to register with the government?
    - Does the government require that individuals use their real names or register with the authorities when posting comments or purchasing electronic devices, such as mobile phones?
    - Do specific laws or binding legal decisions require digital platforms, content hosts, or other intermediaries to identify or verify their customers' real names?
    - Are individuals prohibited from using encryption services or other tools to protect their communications or to facilitate private web browsing (as with virtual private networks that encrypt web traffic)?
    - Do specific laws or binding legal decisions undermine strong encryption protocols, such as mandates for traceability or real-time monitoring, or requirements that decryption keys be turned over to the government?

5. **Does state surveillance of internet activities infringe on individuals' right to privacy?** (*0–6 points*)
    - Does the constitution, specific laws, or binding legal decisions protect against government intrusion into private lives?
    - Do state actors comply with these laws or legal decisions, and are they held accountable, including by an independent judiciary or other forms of public oversight, when they do not?
    - Do state authorities engage in the blanket collection of communications metadata and/or content transmitted within the country?

- Are there legal guidelines and independent oversight on the collection, retention, and inspection of surveillance data by state security and law enforcement agencies, and if so, do those guidelines adhere to international human rights standards regarding transparency, necessity, and proportionality?
- Do state authorities monitor publicly available information posted online (including on websites, blogs, social media, and other digital platforms), particularly for the purpose of deterring activities protected under international human rights standards such as independent journalism, community building and organizing, and political, social, cultural, religious, and artistic expression?
- Do authorities have the technical capacity to regularly monitor or intercept the content of private communications, such as email and other private messages, including through spyware and extraction technology?
- Do state actors use artificial intelligence and other advanced technology for the purposes of online surveillance, without appropriate oversight?
- Do state actors manually search people's electronic devices, including while in detention, for the purposes of ascertaining their online activities or their personal data, without appropriate oversight?
- Do government surveillance measures target or disproportionately affect dissidents, human rights defenders, journalists, or certain ethnic, religious, gender, LGBT+, migrant, diaspora, and other relevant groups?

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

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

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

- Are individuals subject to physical violence—such as murder, assault, torture, sexual violence, or enforced disappearance—in relation to their online activities, including membership in certain online communities?
- Are individuals subject to other intimidation and harassment—such as verbal threats, travel restrictions, nonconsensual sharing of intimate images, doxing, or property destruction or confiscation—in relation to their online activities?
- Are individuals subject to online intimidation and harassment specifically because they belong to a certain ethnic, religious, gender, LGBT+, migrant, diaspora, or other relevant group?
- Have online journalists, commentators, or others fled the country, gone into hiding, or undertaken other drastic actions to avoid such consequences?
- Have the online activities of dissidents, journalists, bloggers, human rights defenders, or other individuals based outside the country led to repercussions for their family members or associates based in the country (i.e., coercion-by-proxy)?

8. **Are websites, governmental and private entities, service providers, or individuals subject to widespread hacking and other forms of cyberattack?** (*0–3 points*)
    - Have websites belonging to opposition, news outlets, or civil society groups in the country been temporarily or permanently disabled due to cyberattacks (such as distributed denial-of-service attacks), particularly at politically sensitive times?
    - Are websites, news outlets, blogs, or social media accounts subject to targeted technical attacks as retribution for posting certain content, for example on political and social topics?
    - Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks meant to steal data or disable normal operations, including attacks that originate outside the country?
    - To what extent do specific laws, policies, or independent bodies prevent and protect against cyberattacks (including systematic attacks by domestic nonstate actors)?

Acknowledgements and Sources

Freedom on the Net is a collaborative effort between Freedom House and a network of experts from civil society organizations, academia, journalism, and other backgrounds. For experts working in repressive environments, Freedom House ensures anonymity in order to protect their safety.

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

Freedom on the Net 2025 was made possible by the generous support of the Dutch Ministry of Foreign Affairs, The Dutch Postcode Lottery, Google, Internet Society, Internet Society Foundation, The New York Community Trust, and Proton. This list includes general support and project-specific funding. All US-related research and activities are funded by US-based private donations.

The US State Department's Bureau of Democracy, Human Rights, and Labor (DRL) provided funding for the project through a multiyear grant that was terminated on March 4, 2025, as part of a broader freeze on US foreign assistance that began in January 2025. Freedom House used alternative funding sources to continue the project.

Freedom House is committed to editorial independence. Our donors have no influence over the content of our publications. All findings and recommendations herein reflect only our own research, judgment, and perspective.

CONTRIBUTORS

Freedom House staff

- **Allie Funk**, Research Director for Technology and Democracy
- **Jennifer Brody**, Deputy Director of Policy and Advocacy for Technology and Democracy
- **Cathryn Grothe**, Senior Research Analyst for Democracy Studies
- **Amy Slipowitz**, Research Manager, Free Them All: The Fred Hiatt Program to Free Political Prisoners
- **Kian Vesteinsson**, Senior Research Analyst for Technology and Democracy
- **Grant Baker**, Research Analyst for Technology and Democracy

Shannon O'Toole and Tyler Roylance edited *Freedom on the Net*. Gerardo Berthin, Annie Boyajian, Yana Gorokhovskaia, Katie LaRoque, and Adrian Shahbaz provided valuable feedback on the summary of findings. Former Freedom House staff Aashna Agarwal, Matthew Barak, Mina Loldj, Maddie Masinsin, Michael Smeltzer, and Elizabeth Sutterlin were instrumental to the research process.

Independent experts

- **Mila Bajić and Bojan Perkov**, SHARE Foundation
- **Atnafu Brhane Ayalew**, independent researcher
- **Digital Rights Lab Sudan**
- **Conor Fitzpatrick**, Foundation for Individual Rights and Expression (FIRE)
- **Arzu Geybulla**, independent researcher
- **Katie Harbath**, Anchor Change
- **Jennifer Huddleston**, Cato Institute
- **Human Rights Myanmar**
- **Khalid Ibrahim**, Gulf Centre for Human Rights
- **Olga Kyryliuk**, digital policy and governance strategy
- **Rachel Levinson-Waldman**, Brennan Center for Justice
- **Artur Pericles Lima Monteiro**, Yale Law School and Yale Jackson School of Global Affairs
- **Lillian Nalwoga**, independent researcher
- **Bulanda T. Nkhowani**, independent researcher
- **Gürkan Özturan**, European Centre for Press and Media Freedom (ECPMF)
- **Smitha Krishna Prasad**, Georgetown University Law Center
- **Iria Puyosa**, Democracy + Tech Initiative, Atlantic Council
- **Vladimir Cortés Roshdestvensky**, independent researcher
- **Southeast Asia Freedom of Expression Network** (SAFEnet)

Independent experts from Bangladesh, Georgia, Kyrgyzstan, and Russia wished to remain anonymous.

A NOTE ON ADDITIONAL SOURCES AND DATA

This report's main essay, data points, and policy recommendations were informed by research for *Freedom on the Net's* summaries of country-specific developments, which benefited from the perspectives of the independent experts listed above. Freedom House also extends appreciation to the organizations and individuals who advised on country-specific developments, particularly the Internet Society and its chapters.

Country-specific data can be downloaded at freedomonthenet.org, and each summary of country-specific developments is available at https://freedomhouse.org/countries/freedom-net/scores.

HOW TO CITE THIS REPORT

Vesteinsson, Baker, Brody, Funk, Grothe, Slipowitz eds. *Freedom on the Net 2025*, Freedom House, 2025, www.freedomonthenet.org.

Vesteinsson and Baker, "An Uncertain Future for the Global Internet," in Vesteinsson, Baker, Brody, Funk, Grothe, Slipowitz eds. *Freedom on the Net 2025*, Freedom House, 2025, www.freedomonthenet.org.

"Angola," in Vesteinsson, Baker, Brody, Funk, Grothe, Slipowitz eds. *Freedom on the Net 2025*, Freedom House, 2025, www.freedomonthenet.org.

Freedom House is a nonprofit, nonpartisan organization that works to create a world where all are free. We inform the world about threats to freedom, mobilize global action, and support democracy's defenders. Freedom House is not affiliated with any political party and does not engage in any campaign activity for or against any political candidate.

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

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