

FREEDOM ON THE NET 2026

Seismic Shifts on the Global Internet



Highlights from Freedom House's annual report on internet freedom

FREEDOM ON THE NET 2026

TABLE OF CONTENTS

Key Findings	1
<i>Freedom on the Net 2026: Seismic Shifts on the Global Internet</i>	2
A new era of digital isolation	3
Age-gating transforms the internet	7
Government transitions drive improvements	14
Freedom on the internet of the future	17
Policy Recommendations	24
What We Measure	26
Checklist of Questions	27
Acknowledgements and Sources	33

TABLES, CHARTS, AND GRAPHICS

How Free Are the World's Internet Users?	2
Long-term Internet Blackouts Intensify Crises	4
Internet Freedom Under Pressure in Democracies	10
AI Regulation Starts with Internet Content	12
Mass Mobilization Powered by Young People	16
<i>Freedom on the Net 2026 Map</i>	18
Global Rankings	20
Regional Rankings	22

This report was made possible by the generous support of the Dutch Ministry of Foreign Affairs, Google, Internet Society, and The New York Community Trust, as well as through Freedom House's [partnership](#) with Rutgers Democracy Lab (RDL).

Yana Gorokhovskaia, Cathryn Grothe, Amy Slipowitz, and Grady Vaughan were instrumental in the research and writing of this report. Shannon O'Toole edited the booklet and Jennifer Brody authored the policy recommendations. Jamie Fly and Katie LaRoque provided valuable input.

Freedom House is committed to editorial independence. This report's content is solely the responsibility of the staff of Freedom House and does not represent the views or opinions of its board members or donors. The reporting period for *Freedom on the Net 2026* is June 1, 2025—May 31, 2026.

This booklet is a summary of findings for the 2026 edition of *Freedom on the Net*. Summaries of developments in the 38 countries assessed in this study can be found on our website at freedomonthenet.org.

ON THE COVER

Iranian demonstrators in Washington, DC protest the Iranian government's internet shutdown. (Photo: Ali Khaligh/ZUMA Press Wire)

Key Findings

1

Global internet freedom declined for the 16th consecutive year. Iran joined the world's worst environments for internet freedom and marked the most significant deterioration during the coverage period, as authorities brutally repressed an antigovernment protest movement in January and enacted extreme online censorship after the United States and Israel attacked the country in February, starting a monthslong war. China and Myanmar remained among the world's worst environments, while Estonia was the freest online environment.

2

Authoritarians advanced efforts to isolate their populations from the global internet. Iranian authorities imposed the longest nationwide internet shutdown *Freedom on the Net* has ever recorded, and restructured internet services in the country so that only a privileged few could access global platforms. In Russia, President Vladimir Putin consolidated control over internet service providers (ISPs) to maintain access to state-approved websites during internet shutdowns, as authorities enacted connectivity restrictions across the country.

3

Age assurance is reshaping the internet, as laws mandating age checks for social media use take effect around the world. Policymakers have pursued these measures at full speed since Australia's under-16 social media ban, the first in the world, took effect in December 2025. As the laws entered into force, people encountered new barriers to online content and new risks to privacy and security. The world's repressive leaders have already sought to leverage so-called age-gating mandates for their own ends, such as invasive online surveillance.

4

Policymakers took narrow approaches to challenges posed by AI-generated content, addressing meaningful problems but raising concerns about overreach in some countries. During the coverage period, policymakers advanced measures to address artificial intelligence (AI)-enabled impersonation, harassment, and child protection. These narrowly tailored frameworks aim to address concrete policy problems. However, government actors abused some laws in ways that curtailed online expression.

5

The ouster of repressive leaders has led to strong improvements in internet freedom. Bangladesh notched the largest improvement for the second year in a row as the country carried out reforms in the aftermath of the removal of Sheikh Hasina, whose decade-long rule was marked by expansive censorship and surveillance. The Gambia continued its steady gain in internet freedom since the ouster of its own repressive leader Yahya Jammeh almost a decade ago.

6

Internet freedom should serve as a guidepost in the AI era. The rapid adoption of agentic AI services, which perform tasks independently, is already transforming the internet. Around the world, societies will grapple with how to configure the internet in response. Those efforts should work to preserve open exchange and free expression as fundamental values.

Freedom on the Net 2026: Seismic Shifts on the Global Internet

By Kian Vesteinsson

The shape of the internet is changing, as governments across the ideological spectrum erect new barriers to how people access information and express themselves online. Authorities in Iran and Russia accelerated efforts to cut connections to the global internet over the past year, advancing a playbook for how repressive governments can isolate their populations in the digital era. Countries around the world implemented new measures to age-gate access to social media platforms, introducing a landmark change in how platforms operate and introducing new privacy and security risks.

Global internet freedom declined for the 16th consecutive year amid these significant shifts. During this report's coverage period, from June 2025 through May 2026, conditions deteriorated in 16 of the 38 countries assessed, while 8 countries registered overall gains. The year's largest decline occurred in Iran, which joined China and Myanmar as the world's worst environments for internet freedom. Other significant declines were marked in Jordan, where

the government cracked down on online discussion of conflicts in the region, and Nigeria, because of months-long localized internet disruptions affecting parts of Zamfara State. Bangladesh earned the largest improvement, followed by the Gambia, while Estonia was the freest online environment. Georgia's status changed from Free to Partly Free, as authorities continued to suppress online activism and speech perceived to be critical of the ruling Georgian Dream party.

Freedom House paused coverage of 34 countries in this edition of *Freedom on the Net*. The 38 countries covered by *Freedom on the Net 2026* were selected to assess a range of environments across geography, regime types, and types of internet controls. Please consider making a [donation](#) to *Freedom on the Net* to support essential research on threats to freedom online.

HOW FREE ARE THE WORLD'S INTERNET USERS?

Freedom on the Net 2026 assesses 70.9 percent of the world's internet user population.

% of total global internet users, by FOTN status



A new era of digital isolation

For years, the world's most repressive governments have been working to separate people in their countries from the global internet, a phenomenon known as "[internet fragmentation](#)." These efforts accelerated during the coverage period as authoritarians imposed severe censorship measures and prevented people from circumventing them. In Iran and Russia, expansive internet shutdowns, state-backed alternatives to censored platforms, and restrictions on commercial anticensorship technology point to the adoption of a harsher, more aggressive playbook for digital isolationism.

While Iranian authorities have long carried out repressive internet shutdowns, this year marked a further reconfiguration of the Iranian internet into a two-tiered system where most people are cut off from the global internet and only a privileged few are able to freely connect. This tiered internet system enabled Iranian authorities to maintain a stranglehold on online information amid successive crises but also to cater to the country's elites, who still enjoy the benefits of the global internet.

In January 2026, demonstrations that had begun in Tehran over deteriorating economic conditions and dissatisfaction with the government spread across the country, organized partly through social media. In response, Iranian authorities killed thousands of people (with some estimates extending to 30,000 deaths) and imprisoned around 50,000, including some who had simply posted on social media to criticize authorities or support the protesters. Amid this wave of violent repression, the government imposed a near-total internet shutdown for 20 days to suppress the outpouring of popular dissent.

In February, Iranian authorities initiated the longest nationwide internet shutdown in *Freedom on the Net*'s 16 years of publication, as the United States and Israel launched military strikes against the country. For approximately 88 days, the majority of Iran's population was prevented from accessing the internet, even as missiles dropped across the country. By May, telecommunications providers began offering Iranians "Internet Pro" packages to connect to the global internet, which were five times the cost of conventional service and required subscribers to consent to surveillance by authorities. The Iranian government also

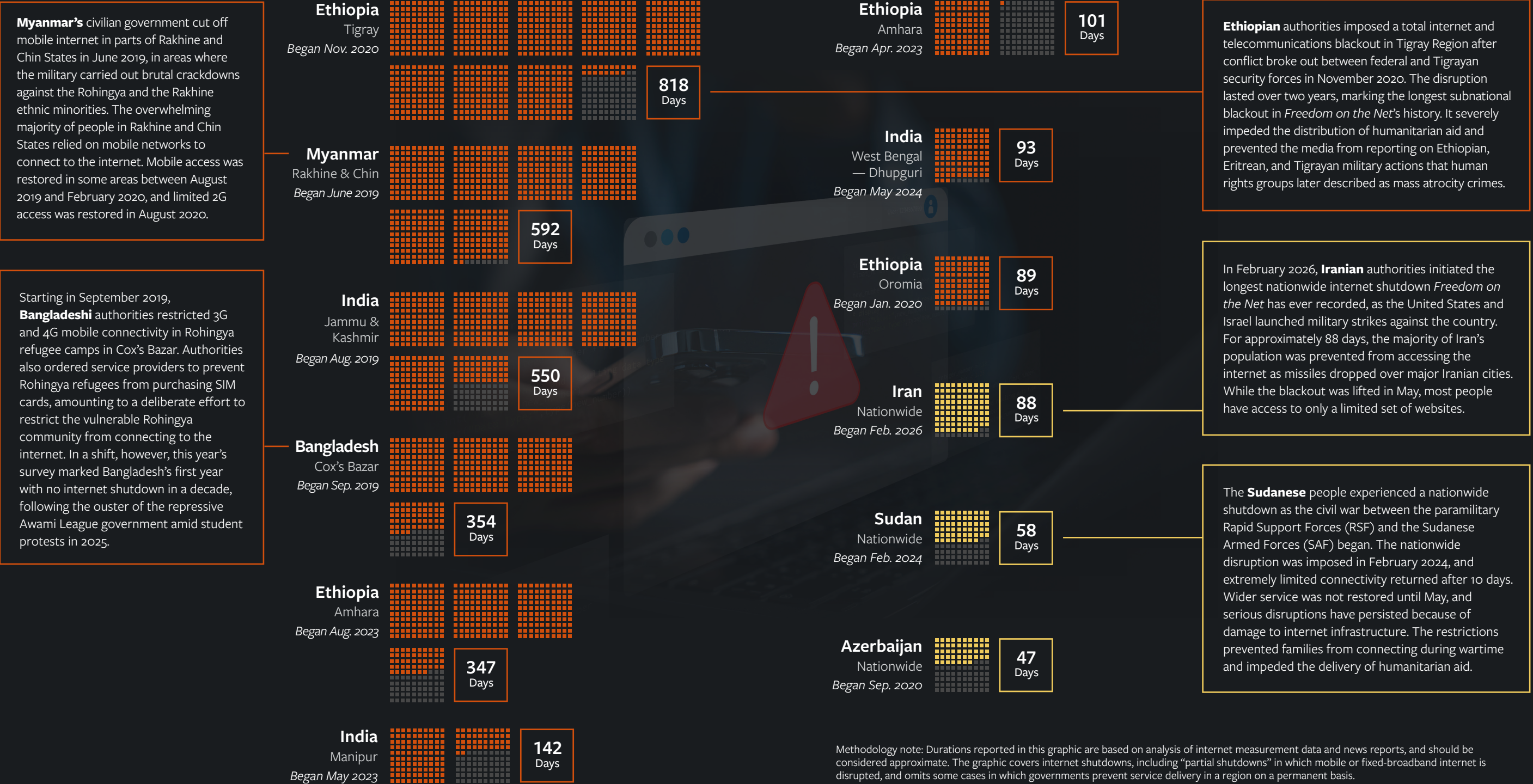
fought circumvention of the blackout, raising the prices of state-backed virtual private networks (VPNs), jamming signals from the satellite provider Starlink, and, in at least one case, violently arresting a man alleged to possess a Starlink terminal, resulting in his death.

Russian authorities also moved to sever the country from the global internet while maintaining public access to state-approved internet services. In September 2025, authorities introduced a "register of socially significant services" to which internet providers should maintain access during shutdowns, including state media outlets, state-aligned platforms like VK and Odnoklassniki, and the state-owned messenger Max. The government passed new rules in November that identified "external information influences" as a threat to the Russian internet and authorized the communications regulator Roskomnadzor to carry out a range of censorship measures in response. In February, the government passed a law authorizing the Federal Security Service (FSB) to enact shutdowns on receipt of a presidential decree—effectively empowering Vladimir Putin to shut down the internet for any reason.

The slate of Russian censorship laws was accompanied by an escalation of technical restrictions on the internet. Authorities enforced extensive short-term mobile internet shutdowns across the country around the commemoration of the Victory Day holiday in May 2026, and people reported that even websites listed as "socially significant services" were not accessible during the restrictions. Longer-term restrictions on mobile internet were also reported, including a 19-day shutdown in Moscow in March 2026. In November 2025, authorities restricted mobile internet in parts of Ulyanovsk Oblast, which officials stated would last until the end of the "special military operation," the term Russian authorities use to refer to the full-scale Russian military invasion of Ukraine. The impacts of these shutdowns were exacerbated by escalating restrictions on VPNs, which can be used to sidestep internet censorship. In March, authorities reportedly instructed ISPs to bar access to people using VPNs, and the research group RKS Global soon after found that many mainstream Russian services were surveilling users for indicators of VPN traffic.

Long-term Internet Blackouts Intensify Crises

Iranian authorities cut off internet access nationwide for 88 days, joining the ranks of the longest shutdowns *Freedom on the Net* has recorded. Many were enforced during brutal conflicts and government crackdowns, carrying a steep human cost.





A Russian Interior Ministry officer takes a photo of an activist protesting against a new censorship law near the State Duma in July 2025. Russian authorities expanded censorship powers during the coverage period. (Photo: Yulia Morozova via Reuters)

Other governments introduced new efforts to disconnect people from the global internet. In Kyrgyzstan, where authorities have increasingly persecuted independent media, President Sadyr Japarov enacted a novel measure granting a state-run ISP a monopoly on international internet traffic. Under a July 2025 presidential decree, all service providers

in the country were required to route international internet traffic to the telecommunications company ElKat, which Kyrgyzstani authorities had nationalized earlier that month. The ability to force all traffic through a state-controlled entity effectively enables the authorities to surveil and censor with ease. While the original decree specified that this “temporary monopoly” would last for a one-year period starting in August 2025, authorities proposed extending it at the end of that term, in August 2026.

As authoritarians pursue internet fragmentation as a method of political control, the global internet offers a precious space for people living under repression to access independent information and express themselves freely. In these contexts, technology that enables people to sidestep government censorship becomes a lifeline. Investments in anticensorship innovation and service delivery are sorely needed to ensure that that lifeline reaches those who need it most.

The global internet offers a precious space for people living under authoritarian repression to access independent information and express themselves freely.

Age-gating transforms the internet

Governments around the world have advanced policies to prevent minors from accessing certain internet content, usually citing concerns about children’s safety and mental health. Policymakers in 10 of the 38 countries covered by FOTN had proposed, passed, or implemented age-assurance laws for social media platforms or other nonpornographic online content as of June 2026. Age-assurance mandates require services to deploy certain methods to assess the likely age of users, including methods that involve the collection

of sensitive personal data like face scans and photos of government identification. While protecting children online is an important policy aim, the first wave of age-assurance laws presented new risks for privacy and security and threatened [online anonymity](#).

Australia’s under-16 social media ban, the first of its kind, entered into force in December 2025. The law requires covered platforms to take “reasonable steps” to verify the

WHAT IS AGE ASSURANCE AND HOW DOES IT WORK?

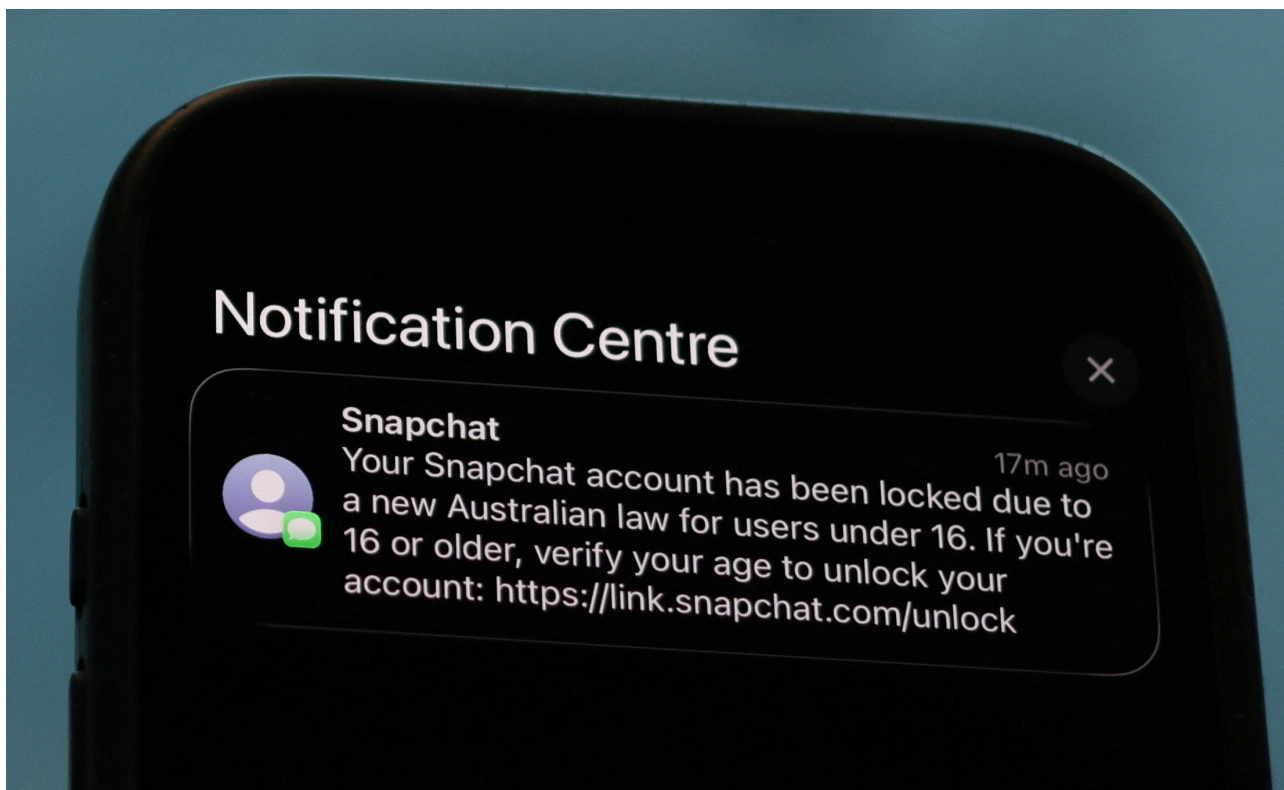
“Age assurance” describes methods and technologies that internet services, including websites or social media platforms, use to assign, estimate, or verify a user’s age. As governments around the world adopt laws designed to protect children on the internet, performing age assurance in a privacy-protecting way has become a pressing rights and cybersecurity issue.

Age-assurance laws require internet services to confirm a user’s self-attested age. The methods currently available for age assurance rely on previous mass data collection or involve processing sensitive information. Because the process can be technically complicated and expensive, many companies contract all or some age-assurance functions to third-party providers to manage costs, convenience, and legal liability.

The largest social media platforms collect extensive data from their users and are able to deploy “age estimation” or “age inference” techniques: trawling and analyzing data for behavioral patterns or other signals that indicate whether a user is an adult or a minor. This is possible when a service retains data that can be analyzed to estimate a user’s age, such as the content of queries and the lifespan of an account. Companies can also purchase data collected by data brokers or signals from another third party, like credit card companies, to attempt age estimation.

Other methods require the provider to capture and analyze sensitive personal information. Companies can estimate a person’s age through face analysis, which entails scanning a photo of the user’s face for indicators of age, like facial hair or wrinkles; this method often results in false positives for older teens and false negatives for young adults. Companies can also process a government-issued identification card, a method called “age verification,” which often requires a face photo for identity verification purposes.

The cybersecurity risks of age assurance only grow when a third-party company is involved. For example, the social platform Discord disclosed in October 2025 that a third-party customer service vendor had been compromised. The vendor processed requests from Discord users to challenge the platform’s age-estimation results through age verification, and 70,000 government ID photos collected for those appeals may have been exposed in the breach.



A notification from Snapchat prompting an age check because of Australia's under-16 social media ban. Early surveys indicate that teens have evaded the ban at significant rates, sometimes by manipulating age-estimation and age-verification algorithms. (Photo: Hollie Adams via Reuters)

age of users and prevent those under the age of 16 from creating or owning accounts; guidance from Australia's eSafety commissioner set out a range of methods deemed to be reasonable steps. Australian officials designated 10 major social media platforms—including Facebook, Instagram, Snapchat, and TikTok—as covered by that law, while several other companies voluntarily complied, such as major dating services. The law sets out privacy preservation and data minimization (collecting only what is deemed necessary data) as principles to guide the implementation of age-gating.

Initial implementation of the law resulted in the mass deletion of accounts—around 5 million as of March 2026, according to the eSafety commissioner—though broader impacts on freedom of expression and access to information were not clear. Early surveys and news reports indicate that teens have evaded the ban at significant rates, sometimes by manipulating age-estimation and age-verification algorithms. Eighty-five percent of children under 16 surveyed in one early study reported that they continued to use social media platforms after the ban; some may have circumvented or supplied false information to age checks to retain access, as

one-fifth of those surveyed reported submission of a face photo and one-tenth reported use of a government ID as part of an age-assurance process. Another study found over 60 percent of 14- and 15-year olds surveyed were still using social media, some 57 percent of whom said they manipulated age-verification checks to maintain access.

Indonesian lawmakers passed and implemented an under-16 social media ban in March 2026, applying to “high-risk” platforms. The government had previously passed an age-assurance framework that adopted a risk-categorization approach, requiring companies to assess whether their platforms had features deemed “high risk” for children, like contact with strangers or pornographic content. Indonesian officials stated that some 4.7 million accounts were deleted by June, 4.1 million deletions of which were reported by TikTok. Meanwhile, Indonesian authorities have significantly lagged in implementing the country's data-protection law, and civil society organizations in the country raised concerns that the rapid implementation of age-assurance methods would expose children's data, such as face or identification photos, to new risks.

In the United States, a patchwork of state-level laws illustrates the tension between age-assurance laws and protections for freedom of expression. Nineteen of 50 states had passed a social media age-gating law as of June 2026, though implementation of most of them was paused in response to lawsuits. In most cases, district courts found that social-media-focused age-assurance laws would likely violate the First Amendment on the basis that they require differential treatment for different forms of online content (that is, the laws create a burden for websites featuring certain kinds of content, like social networking, and exempt others, like professional networking).

In contrast, the Supreme Court ruled in the June 2025 *Free Speech Coalition v. Paxton* case that a Texas law mandating age verification for websites hosting “speech that is obscene to minors” did not violate the First Amendment. The court’s ruling in *Paxton* affirms the many state-level age-gating requirements for adult content. In March 2026, Utah passed a law that required adult website hosts to analyze traffic to determine whether Utah-based visitors had employed VPNs to evade the state’s law mandating age assurance for adult content. The technology used by commercial VPNs is deployed widely for privacy and security, and the Utah law poses serious risk that website hosts would be forced to treat encrypted internet traffic as suspect.

Age-assurance laws also open a new potential vector for abuse, with identification requirements enabling bad actors and repressive governments to create a footprint of people’s online activities. Turkey’s parliament passed a bill in April 2026 that would restrict children under 15 from social media platforms, though it was not fully approved by the end of the coverage period. The bill would enforce age-gating for social media platforms solely through the e-Devlet portal, a government-run digital identity system, effectively tying all social media accounts to individuals’ real names. People in Turkey are routinely arrested and imprisoned over their online expression, particularly for criticism of President Recep Tayyip Erdoğan, and the proposed e-Devlet age-assurance

framework poses significant risks for Turkish citizens who turn to the internet to discuss problems in their country.

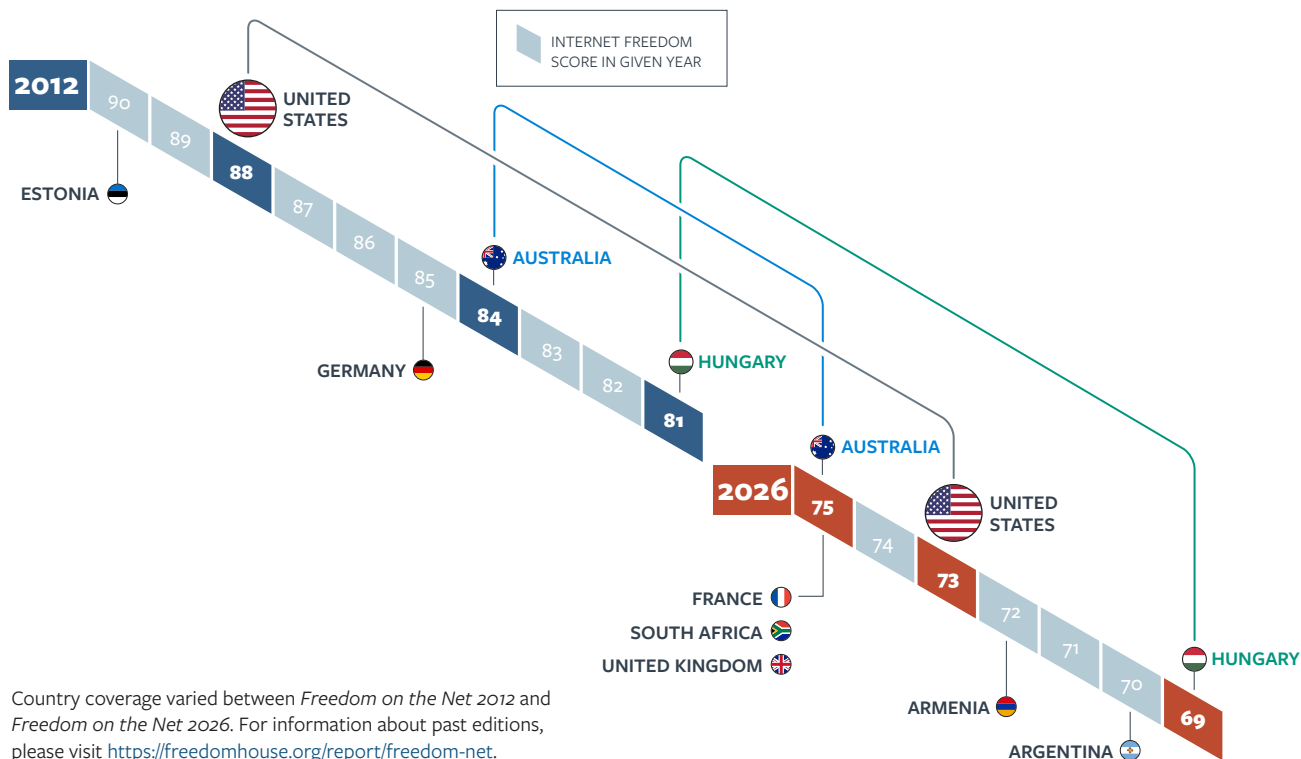
The Chinese Communist Party (CCP) has adopted the language of child protection in its long-standing efforts to erode anonymity on the Chinese internet. Chinese authorities have mandated real-name registration for internet services since at least 2012 as part of the CCP’s repressive censorship regime. In June 2025, Chinese officials promulgated a draft regulation that sets out a laundry list of “harmful” information that internet services should be required to suppress for minors, largely aligned with the maintenance of CCP narratives about its own governance and China’s place in the world.

The speedy adoption of age-assurance social media bans represents the most significant live experiment in internet regulation in years, and the consequences for internet freedom demand due consideration. The current state of age-inference and age-verification technology, for example, cannot mitigate the privacy and security risks introduced by their large-scale use; further technical research is needed to advance age-assurance methods that are truly privacy-preserving. Meanwhile, children have evaded age-assurance mechanisms at considerable scale, remaining connected to social media platforms that are still rife with problems of the digital age. A rights-respecting pursuit of child safety requires action by policymakers and the private sector to resolve the long-standing problems of the social internet.

Age-assurance laws open a new potential vector for abuse, with identification requirements enabling bad actors and repressive governments to create a footprint of people’s online activities.

INTERNET FREEDOM UNDER PRESSURE IN DEMOCRACIES

People in the world's democracies have long enjoyed robust conditions for freedom online. In the past 15 years, however, conditions in some countries have deteriorated.



The United States scored 73 out of a possible 100 points in *Freedom on the Net* 2026. While the score did not change this year, restrictions on civic space that drove a three-point decline in the previous edition have persisted.

Federal authorities continued to exert pressure on digital activism and other online speech expressing criticism of the government. For example, federal law enforcement carried out extensive surveillance of online activists mobilizing in response to the presence of Immigration and Customs Enforcement (ICE) agents in Minnesota, and prosecuted online journalists who reported on those protests.

US officials continued to enforce steeper penalties on people for their online activities than in previous years. In one case, Tennessee police arrested and jailed a man for 37 days after he posted a meme on Facebook that made light of the murder of conservative activist Charlie Kirk.

The government advanced some positive efforts to address online harms. In May 2026, content-removal provisions of the TAKE IT DOWN Act entered into effect. The law, which President Donald Trump signed the previous year, criminalized the nonconsensual distribution of intimate images, an important step to combatting online sexual abuse. However, the law's content-removal framework was broadly framed in a way that civil society organizations argued may be prone to abuse, particularly its lack of safeguards against false reports.

AI REGULATION IN PRACTICE

Much of the policy conversation about the AI boom has centered around the value of comprehensive regulatory frameworks and safety concerns. Recent regulation has taken a narrower approach aimed at solving particular issues, such as impersonation or harassment. Some measures raised concerns about overreach, such as in India and Mexico, as described below. Broader concerns persist about how AI models can [reinforce censorship practices](#) of authoritarian regimes like those that rule Russia and China.

Child protection: Lawmakers sought to limit children’s access to AI services deemed especially sensitive. For example, Australia’s eSafety commissioner announced in September 2025 that the country’s under-16 age-assurance framework would apply to certain AI companies, particularly those that host “AI companions” designed to simulate friendship or romantic relationships. While the privacy and security risks around age assurance persist, early research on AI companion services indicate they threaten emotional and psychological harms for vulnerable users, particularly minors.

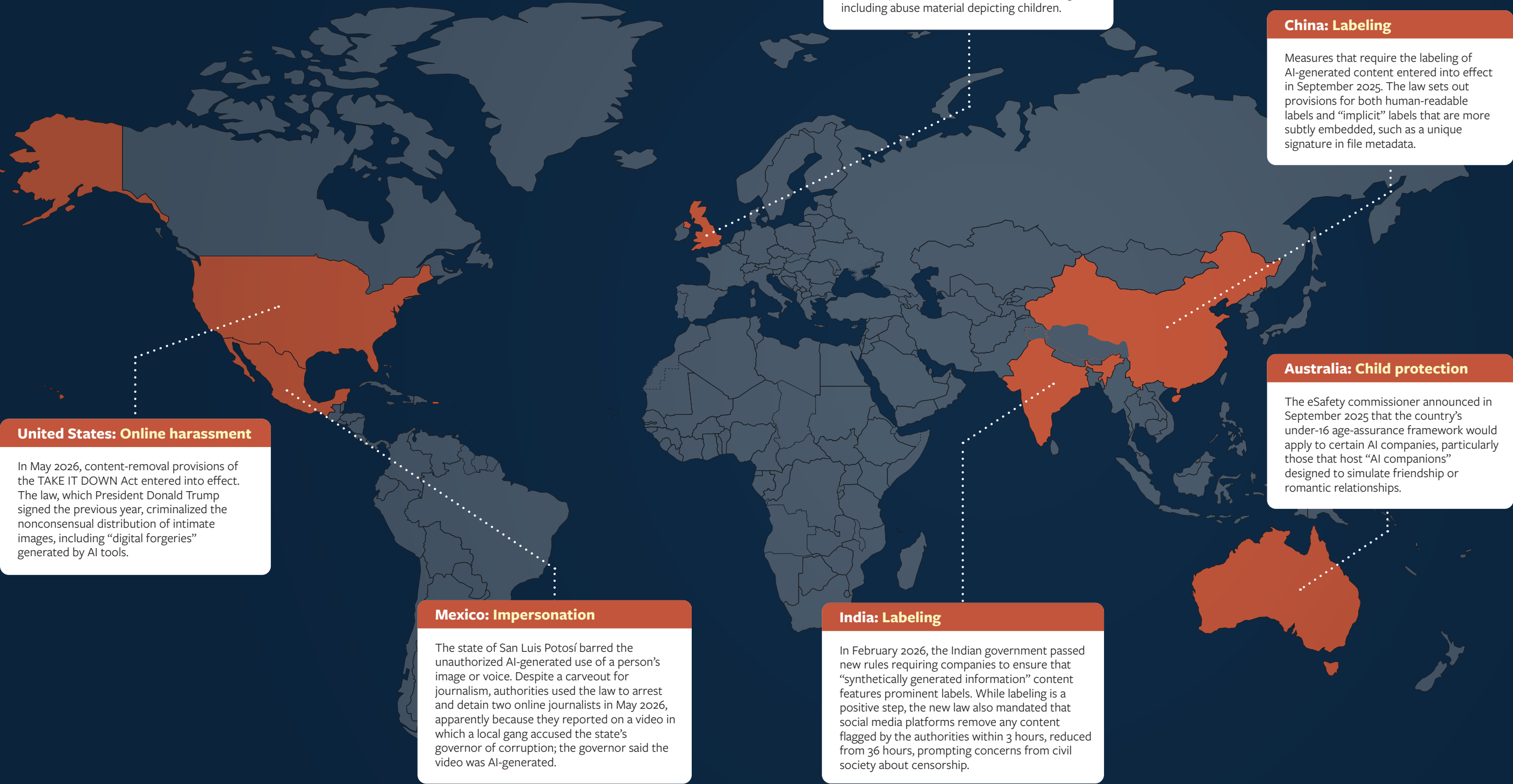
Online harassment: Bad actors abuse AI tools to generate sexual imagery of people without their consent. Governments have rightly taken up efforts to push tech platforms to remove these images and create barriers to their generation. UK authorities amended a law penalizing people who create or commission nonconsensual imagery to include AI tools in February 2026, and launched an investigation into X’s Grok service after the platform failed to remove such images, including abuse material depicting children.

Labeling: In February 2026, the Indian government passed new rules requiring technology companies and social media platforms to ensure that “synthetically generated information” content features prominent labels. While labeling AI-generated content is a positive step, the new law also mandated social media platforms to remove any content flagged by the authorities within 3 hours, reduced from 36 hours under previous law. The Indian government has built expansive infrastructure for internet censorship, prompting concerns from civil society that the new rules would be abused to silence online content deemed unfavorable by the government, including independent journalism and satire, particularly because the 3-hour period limits careful evaluation of reported material, forcing platforms to err on the side of removal.

Impersonation: Policymakers around the world expressed concern about how generative AI tools could be used to impersonate people to cause reputational harm or carry out scams. In some countries, lawmakers sought to criminalize such impersonation. For example, in Mexico, the state of San Luis Potosí reformed the penal code to bar unauthorized AI-generated use of a person’s image or voice, as well as the intentional dissemination of disinformation generated through AI. Despite a carveout for journalism, authorities used the law to arrest and detain two online journalists in May 2026, apparently because they reported on a video in which a local gang accused the state’s governor of corruption; the governor said the video was AI-generated.

AI Regulation Starts with Internet Content

While policy conversation around AI often fixated on comprehensive regulatory frameworks and safety concerns, lawmakers advanced measures to address specific issues relating to online content. Some measures raised concerns about overreach.



Government transitions drive improvements

Improvements in Bangladesh and the Gambia showcased how mass movements that overthrow repressive leaders can drive short- and long-term gains in internet freedom.

Bangladesh marked the strongest improvement in *Freedom on the Net* 2026, as the country's interim government continued to implement an agenda of reforms since a mass uprising ousted former Prime Minister Sheikh Hasina in August 2024. The country saw its first year with no internet shutdown since 2016, marking a stark contrast to Hasina's Awami League (AL) government, which routinely cut off internet connectivity during opposition rallies

and protests including during the 2024 uprising. The new interim government reportedly established a prohibition on the shutdown of telecommunications networks in the Bangladesh Telecommunication (Amendment) Ordinance 2025, passed that December, though the final text of the law has not been published and the legislative process was rushed and nontransparent.

However, the interim authorities also sought to suppress real or perceived support for the AL, sometimes deploying the former government's same repressive tactics. The interim government banned the AL from participating



Demonstrators affiliated with the Bangladesh Nationalist Party attend a rally during the February 2026 general election. The party won the vote and faces significant challenges in building a sustainable democratic transition. (Photo: Syed Mahamudur Rahman/NurPhoto via Reuters)

in the February 2026 general election. More than 280 journalists, some of whom work for online outlets, faced politicized charges as of May 2026, with most cases linked to coverage of the 2024 uprising perceived to be too favorable toward the AL. In December 2025, rumors spread online that accused *Prothom Alo* and *The Daily Star*, the country's two most prominent independent media outlets, of pro-India sentiment—shorthand used as a signifier of support for Hasina—and mobs attacked their offices, burning down the buildings and endangering the journalists who worked there.

The Gambia continued its long-term trajectory of democratic gains in the aftermath of the ouster of Yahya Jammeh nearly a decade ago. The environment for online expression continued to improve, as Gambian officials worked with civil society to loosen the censorship framework of the Jammeh era. While bloggers and online journalists occasionally reported arrests or violence in retaliation for their work in recent years, no such incidents were reported during the coverage period. Separately, the government of President Adama Barrow passed a landmark data-protection law in December 2025, marking another significant legal reform as the Gambia rebuilds its democratic institutions.

Improvements in Bangladesh showcase the gains brought by a mass mobilization reversing long-standing practices of digital repression, though significant challenges to a sustainable democratic transition remain for the country's new government, which assumed power after the longtime opposition Bangladesh Nationalist Party won the February 2026 election. The Gambia, which notched steep improvements in the immediate aftermath of the post-Jammeh transition, offers a model of such an effort. The country's recent trajectory reflects steady efforts to repair its democratic institutions, and offers a lesson in how long-term internet freedom improvements require sustained investment and collaboration with civil society.

The Gambia's steady efforts to repair its democratic institutions offer a lesson in how long-term internet freedom improvements require sustained investment and collaboration with civil society.

Mass Mobilization Powered by Young People

Around the world people used digital tools to mobilize landmark protests, many of them youth-led and oriented around economic issues or antigovernment sentiment.



India

After India's chief justice referred to unemployed young people as cockroaches, an activist launched a satirical social media account called Cockroach Janta Party (CJP). CJP fueled a nationwide movement demanding education and economic reforms. Authorities censored CJP's internet presence and cracked down on protests.



Iran

Protests around the sharp devaluation of Iran's currency evolved into nationwide antigovernment demonstrations in January 2026. The regime used brutal violence to quash the protests, initiated mass arrests and unlawful killings of demonstrators, and enacted a 20-day internet shutdown.



Hungary

Hungarian lawmakers passed a law banning Pride events and authorizing authorities to employ facial-recognition tools to identify people at LGBT+ gatherings. In response, Hungarians mobilized online to coordinate the June 2025 Budapest Pride march, resulting in the largest turnout in the event's history.



Serbia

Serbians continued to mobilize in student-led antigovernment protests sparked by the 2024 collapse of a train station canopy that killed 16 people. The government has harshly repressed the protests, many of which were organized using digital tools.



Kenya

Young Kenyans used social media to organize marches demanding justice for those killed in the June 2024 #RejectFinanceBill protests on the first anniversary of their deaths. The protests were once again met with a crackdown and police brutality.



Cuba

Despite enormous risks to mobilization in Cuba, some dissent persists. After the state-owned telecommunications provider abruptly increased prices in 2025, young Cubans condemned the decision online. Cubans also took to social media to commemorate the anniversary of the July 2021 protests, which authorities had brutally repressed.



Freedom on the internet of the future

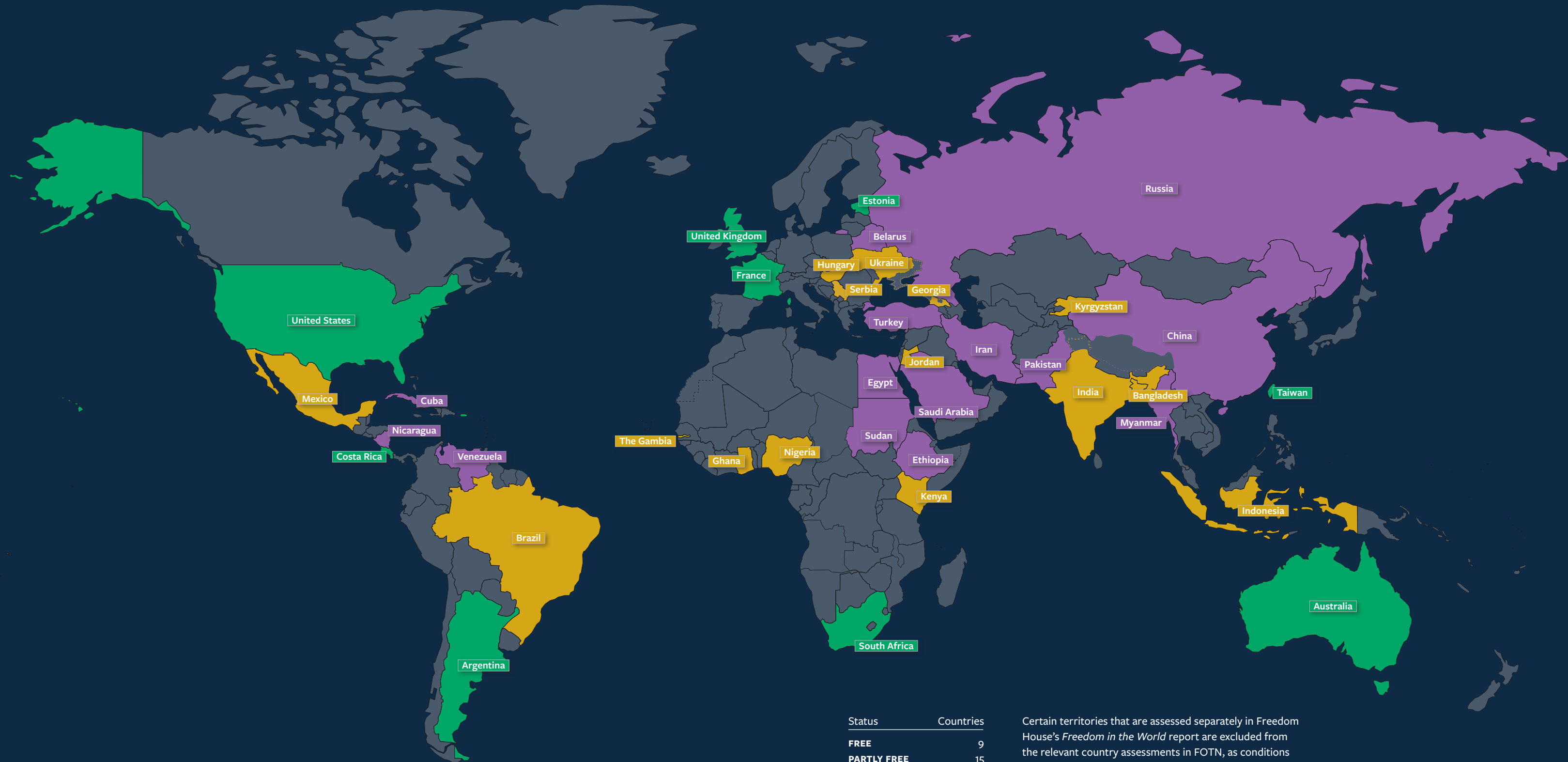
The acceleration of digital isolation as a tool of authoritarian governments and the rapid adoption of age-assurance frameworks pose novel challenges, even as the rise of AI services that perform tasks autonomously promises transformative consequences for the internet. Around the world, societies will grapple with questions about how to ensure that people in repressive environments can stay connected, balance the need to build safer online spaces against the right to free expression, and ensure access to reliable information as AI services become more deeply embedded in daily life.

The societal response to these challenges will shape how people exercise and access their fundamental rights online. New barriers to online spaces and the rapid adoption of AI services threaten to undermine the power of exchange and expression, benefits that have embedded internet services deeply in today's societies. Interconnected networks enable people to learn and speak more freely, building stronger democratic systems even when powerful actors control other sources of information. This is the long vision of internet freedom and should serve as a guidepost for the internet of the AI era.



Young people around the world mobilized landmark protests using digital tools. In India, a nationwide movement for educational and economic reforms adopted the satirical moniker Cockroach Janta Party. (Photo: Adnan Abidi via Reuters)

FREEDOM ON THE NET 2026



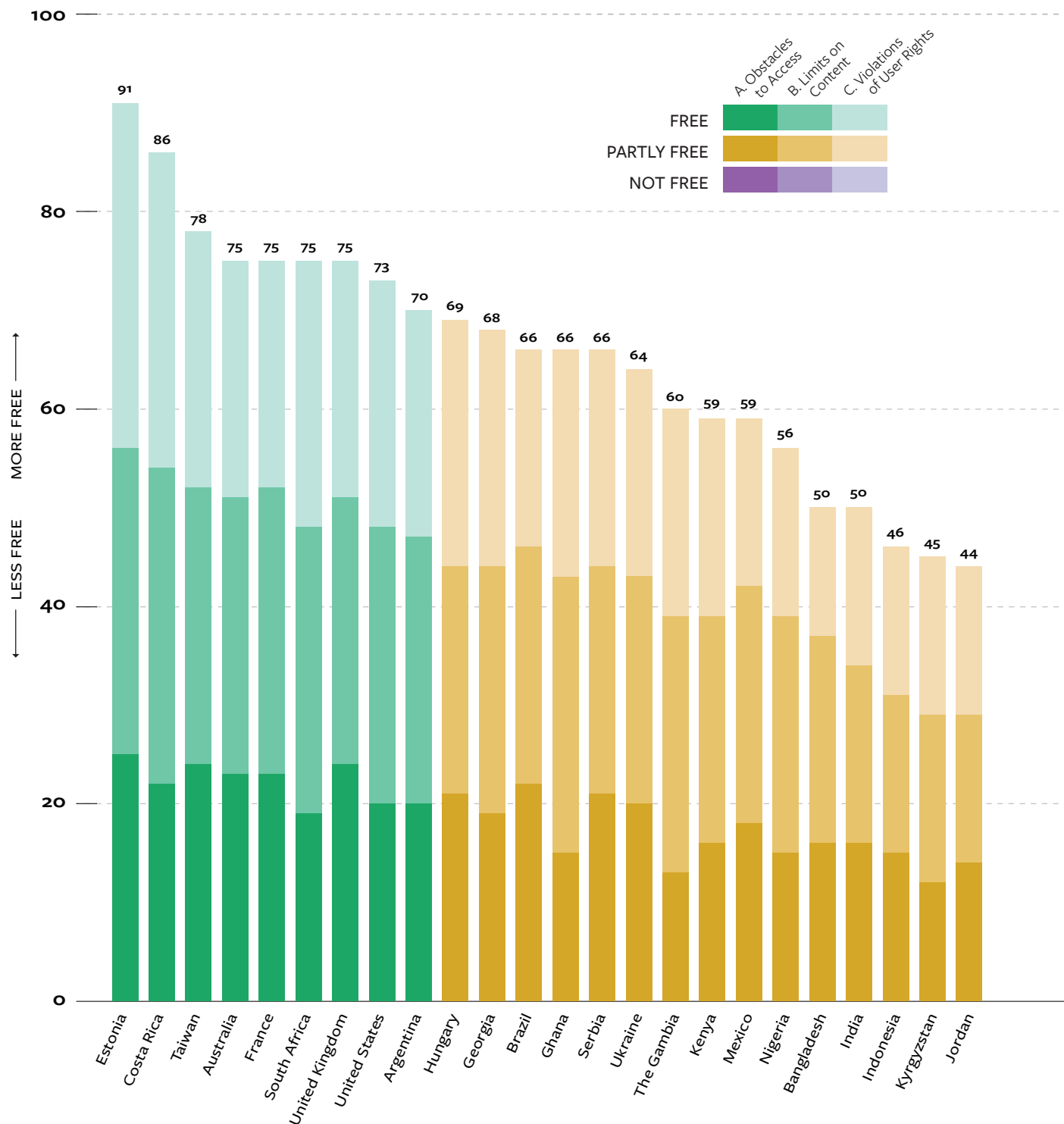
FREE **PARTLY FREE** **NOT FREE** **NOT ASSESSED**

Status	Countries
FREE	9
PARTLY FREE	15
NOT FREE	14
Total	38

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

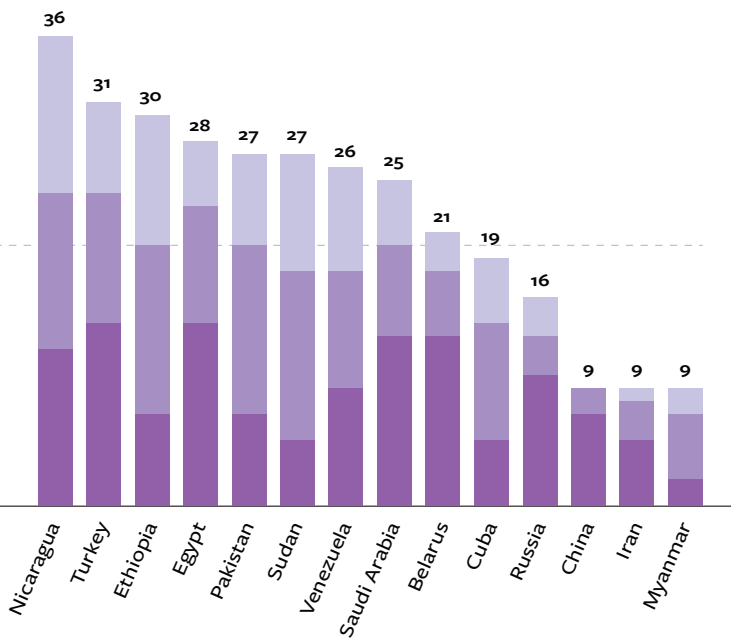
100 = Most Free 0 = Least Free



Freedom on the Net 2026 covers 38 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:

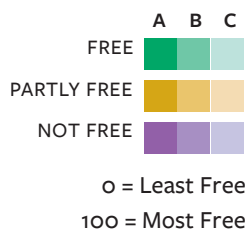
- A. OBSTACLES TO ACCESS:** Assesses infrastructural, economic, and political barriers to access; government decisions to shut off connectivity or block specific applications or technologies; legal, regulatory, and ownership control over internet service providers; and independence of regulatory bodies.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



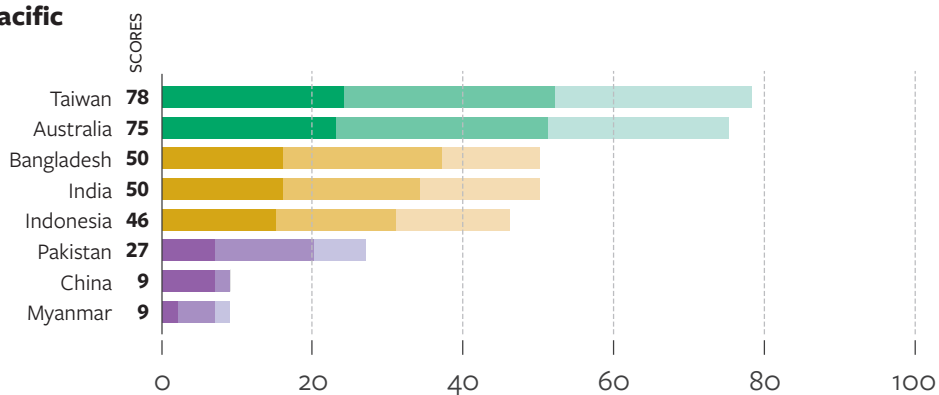
REGIONAL RANKINGS

Freedom on the Net 2026 covers 38 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

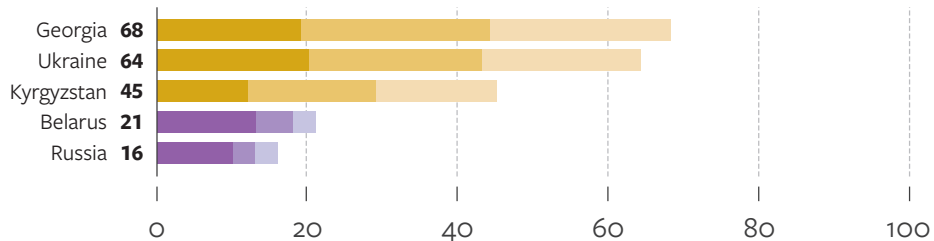
- A. Obstacles to Access
- B. Limits on Content
- C. Violations of User Rights



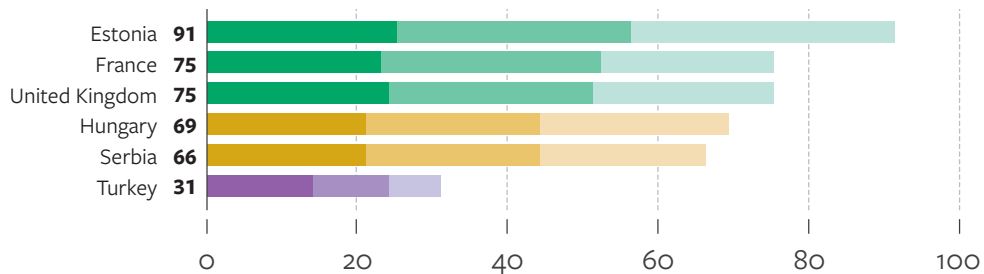
Asia-Pacific



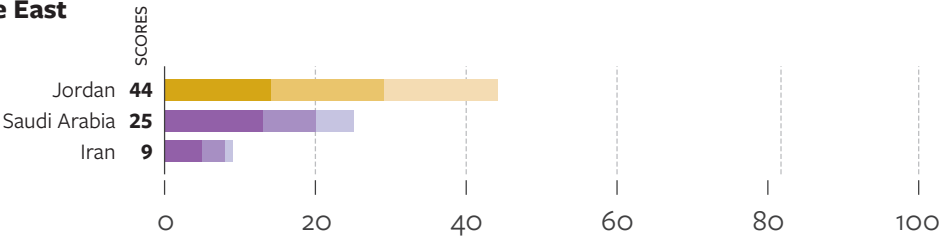
Eurasia



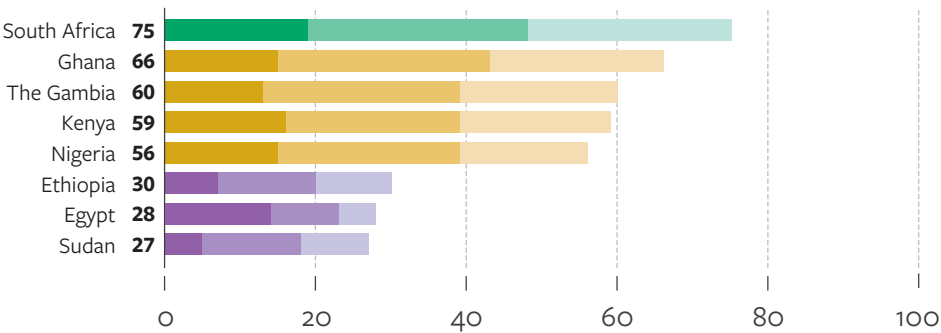
Europe



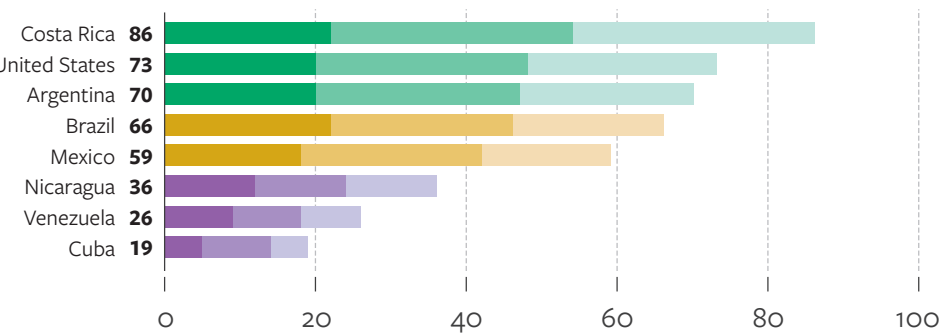
Middle East



Africa



Americas



Policy Recommendations

The fight for democracy in the digital age faces new threats as authoritarians cut their populations off from the global network and as AI technology advances. Democratic governments and the private sector should advance the defense of human rights in the digital age by undermining authoritarian internet restrictions and safeguarding privacy online.

UNDERMINE AUTHORITARIAN INTERNET RESTRICTIONS

Access to the internet is under threat as authoritarian powers continue to create barriers for people to freely express themselves online. Internet shutdowns, throttling, and platform blocking remain among the most common tools of digital repression. At the same time, digital technologies serve as a lifeline for people seeking to expose human rights violations to the outside world and hold dictators accountable.

Combat internet shutdowns. Internet shutdowns are a favored tool of digital repression, deployed by governments during elections, protests, and periods of unrest to suppress dissent and cut off access to the outside world, often with devastating and long-lasting economic and humanitarian consequences.

- Internet service providers should [publicly disclose](#) the shutdown orders they receive and commit to challenging orders they consider disproportionate or unlawful.
- Independent watchdogs should sustain real-time shutdown documentation and rapid-alert initiatives, such as via the #KeepItOn coalition, which tracks and verifies shutdowns worldwide and provides evidence that civil society, journalists, and international bodies rely on to hold governments accountable. To this end, it is imperative that donors continue to support these ongoing efforts.

Support access to satellite internet technologies. These technologies provide a means to circumvent government restrictions on internet access. Supporting access to these technologies takes many forms, including technical investment and diplomatic pressure.

- Governments should conduct [feasibility studies](#) to assess the effectiveness and potential vulnerabilities of nascent Direct-to-Cellular (D2C) satellite internet technologies. They should also evaluate how to safely disseminate the technology and mitigate its exorbitant cost, which may pose barriers to access for human rights defenders on the ground.
- Governments should advocate for access to emergency satellite internet connectivity at the [ITU World Radiocommunication Conference in 2027](#).
- The satellite industry should work closely with civil society to advocate for policies that de-risk satellite internet services, helping ensure that satellite internet providers can continue operating in repressive contexts.

Fund context-specific anticensorship tools. Since the means of censorship vary across different authoritarian regimes, it is necessary to invest in tools that respond to the unique environments in which human rights defenders and journalists are seeking to access the internet.

- The US government should ensure robust funding for the [Open Technology Fund](#), which supports the development of anticensorship tools tailored to human rights defenders and journalists around the world.
- Providers of anticensorship tools should co-develop circumvention tool kits with local civil society organizations as governments introduce new blocking techniques.

Protect against VPN compromise. Virtual private networks (VPNs) provide essential privacy and security services to people around the world and make it possible for those in repressive contexts to safely access the open internet.

- Governments should avoid imposing [age restrictions on VPN use](#), despite legitimate concerns about protecting children. Such policies risk being emulated by authoritarian states with weak rule-of-law institutions, potentially enabling even more severe violations of fundamental rights in repressive contexts.
- Governments should resist [mandates that would require VPN providers to log user activity](#) and VPN providers should resist these demands from governments. Similarly, such requirements would likely be replicated by authoritarian regimes to unmask human rights defenders and journalists.

SAFEGUARD PRIVACY ONLINE

Protecting privacy online is essential to safeguarding free expression in repressive contexts. Without strong privacy protections, journalists and human rights defenders may self-censor out of a fear of reprisal. Rapid advances in AI—and the growing threat of automated vulnerability exploitation—heighten these risks, leaving civil society organizations increasingly vulnerable to sophisticated cyberattacks.

Build accountability mechanisms and normative frameworks to disincentivize the misuse of surveillance tools.

Commercial surveillance technologies are increasingly used by authoritarian governments to surveil human rights defenders, journalists, and political dissidents. Without meaningful consequences, surveillance vendors and their government clients face few disincentives to curb these abuses.

- Governments should use visa restrictions, financial sanctions, and entity listings to [hold surveillance firms accountable](#) when human rights are violated through the misuse of a surveillance tool.
- Export control officers should [improve end-use monitoring](#) of surveillance technologies and [intermediary country oversight](#) to address technology transfer loopholes.
- Democratic governments should support [international norms](#) that seek to combat the misuse of AI to surveil human rights defenders, journalists, and political dissidents.

Assess age-assurance measures for their privacy and security impacts. Online child safety requires urgent attention. However, age-assurance or “age-gating” measures pose privacy and security risks and may introduce barriers to free expression and access to information, particularly those aimed at social media platforms. Policymakers should carefully assess the rights impacts of age-gating and pursue a whole-of-society approach to child safety.

- Funders should invest in technical research to develop age-assurance methods that are truly privacy preserving and mitigate cybersecurity threats.
- Governments should require 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.
- Platforms that permit children to create accounts should provide strong privacy and security safeguards and engage civil society in developing child-protection measures that respect children’s rights.
- Policymakers should strengthen child-specific protections in privacy laws and dedicate additional resources toward [addressing online child abuse](#).

Improve digital security safeguards. Journalists and human rights defenders are frequent targets of sophisticated digital attacks, yet many lack access to the tools and expertise needed to detect and respond to these threats. Strengthening digital security safeguards, from device-level threat notifications to emergency response support, can help close this gap.

- The private sector should ensure that users receive a device notification when their phone is compromised. Apple’s [threat notifications](#) are a best practice that should be emulated by other companies and providers.
- Donors should continue to support [digital security training](#) and [rapid-response help lines](#) for journalists and human rights defenders operating in high-risk environments.

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. 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 2026*. Staff members conducted robust research to analyze developments in the 38 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 on fixed-broadband and mobile connections?
 - Does poor infrastructure (including unreliable electricity) or severe 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?

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, including low Earth orbit satellite internet 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, widely used social media platforms and communication apps?
 - Does the government block, or compel service providers to block, certain protocols, ports, and functionalities within such platforms and apps (for example, Voice over Internet Protocol [VoIP], video streaming, multimedia messaging, or Secure Sockets Layer [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 burdensome legal, regulatory, or economic requirements on the establishment or operation of service providers, including low Earth orbit satellite internet 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, apolitical, and independent from political pressure, and designed to take meaningful notice of comments from stakeholders in society?

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 block or filter websites and online content featuring political, social, cultural, religious, or 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 (such as those related to gambling, pornography, copyright violations, or illegal drugs) 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, 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, censorship-enabling technology, including that which uses artificial intelligence (AI) tools, 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 political, social, cultural, religious, and artistic expression, either prior to or after its publication?
 - Do publishers, digital platforms, or 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 (in other words, 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, internet service providers (ISPs), generative AI systems, and other intermediaries to restrict access to online material, particularly that which is protected under international human rights standards?
 - Are entities 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?
 - 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 other 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, generative AI tools, or other 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 (like search engines, email applications, or 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?
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, and websites represent diverse interests 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 false or misleading content online, including content produced by generative AI tools, significantly contribute to offline harms, such as harassment, property destruction, physical violence, or death?
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 people use generative AI tools to engage in online mobilization?
 - Do state or other actors limit access to online tools and websites (like social media platforms, messaging groups, petition websites, or generative AI tools) for the purpose of restricting free assembly and association online?
 - Does the state use legal or other means (such as criminal provisions, detentions, or surveillance) to restrict free assembly and association online?
 - Does the state use facial or other biometric technologies to identify and apprehend people attending protests that were organized 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 (like 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”; offenses related to 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 purchasing electronic devices, such as mobile phones?
 - Do specific laws or binding legal decisions require digital platforms or other intermediaries to identify or verify users’ real names, including by requiring them to provide a government-issued identity document?
 - Are individuals prohibited from using encryption services, circumvention tools, or other tools to protect their communications or to facilitate private web browsing?
 - Do specific laws or binding legal decisions undermine strong encryption protocols, such as mandates for client-side scanning, traceability, or real-time monitoring?
5. **Does state surveillance of internet activities infringe on individuals’ right to privacy?** (0–6 points)
 - Do 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 AI tools for the purposes of online surveillance, without appropriate oversight?
 - Do state actors manually search people’s electronic devices, including while they are in detention, for the purposes of ascertaining their online activities or accessing 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?
 - 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 (such as service providers, low Earth orbit satellite internet providers, digital platforms, email providers, device manufacturers, and data brokers) without a legal process? Do the country's laws require these companies to collect and retain user data beyond the scope of ordinary business purposes?
 - Are these companies required to store users' data on servers located in the country (that is, are there "data localization" requirements)?
 - Do these companies monitor individuals and supply information about their digital activities to the government or other powerful actors?
 - Does the state attempt to impose similar requirements on these companies through less formal methods, such as threats of censorship and legal liability for company employees?
 - 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 in relation to their online activities?
 - 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 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 (in other words, coercion-by-proxy)?
 - Have foreign nationals in the country been arrested and extradited to their home country in retaliation for their online activity, particularly material that is protected by international human rights standards?
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 or civil society groups or to news outlets in the country been temporarily or permanently disabled due to cyberattacks (such as distributed denial-of-service [DDoS] 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 governmental entities subject to significant and targeted cyberattacks meant to steal data or disable normal operations, including attacks that originate outside the country?

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.

This report was made possible by the generous support of the Dutch Ministry of Foreign Affairs, Google, Internet Society, and The New York Community Trust, as well as through Freedom House's [partnership](#) with Rutgers Democracy Lab (RDL).

Freedom House is committed to editorial independence and is solely responsible for this report's content.

CONTRIBUTORS

Research Team

- **Yana Gorokhovskaia**, Director of Research and Analysis
- **Cathryn Grothe**, Senior Research Analyst for Democracy Studies
- **Amy Slipowitz**, Research Manager for Democracy Studies
- **Grady Vaughan**, Research Analyst
- **Kian Vestinsson**, Deputy Director of Research and Analysis

Shannon O'Toole edited *Freedom on the Net* and the policy recommendations were authored by Jennifer Brody. Jamie Fly and Katie LaRoque provided valuable feedback on the summary of findings. Elizabeth Sutterlin served as a research consultant.

RDL staff Eyal Hanfling and Atl Castro Asmussen advised on the report's findings. RDL interns, including Ashiyana Ahamed, Amanda Goceljak, and Seleena Busi, provided essential research support.

Independent experts

- **Aliya Bhatia**, Center for Democracy & Technology
- **Atnafu Brhane Ayalew**, independent researcher
- **Givi Chanukvadze**, information resilience and digital ecosystems expert
- **Sarkis Darbinyan**, RKS Global
- **Digital Rights Lab Sudan**
- **Eduardo Ferreyra**, independent researcher
- **Olga Kyryliuk**, independent researcher
- **Artur Pericles Lima Monteiro**, Yale Law School and Yale Jackson School of Global Affairs
- **Gürkan Özturan**, European Centre for Press and Media Freedom (ECPMF)
- **Lizzie O'Shea**, Digital Rights Watch
- **Smitha K. Prasad**, Georgetown University Law Center
- **Iria Puyosa**, independent researcher
- **Amir Rashidi**, Miaan Group
- **Vladimir Cortés Roshdestvensky**, independent researcher
- **Southeast Asia Freedom of Expression Network** (SAFE-net)
- **Oliver Spencer**, Human Rights Myanmar

Independent experts from Bangladesh, Jordan, Kyrgyzstan, and the Gambia 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.

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>.



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.

1225 I St NW #1200
Washington, DC 20005

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