Freedom House

FREEDOM ON THE NET 2024

The Struggle for Trust Online

Highlights from Freedom House's annual report on internet freedom

FREEDOM ON THE NET 2024

TABLE OF CONTENTS

TABLES, CHARTS, AND GRAPHICS

This report was made possible by the generous support of the Dutch Ministry of Foreign Affairs, The Dutch Postcode Lottery, Google, Internet Society, The New York Community Trust, the U.S. State Department's Bureau of Democracy, Human Rights, and Labor (DRL), and Verizon.

The following people were instrumental in the research and writing of this report: Aashna Agarwal, Matthew Barak, Jennifer Brody, Cathryn Grothe, Mina Loldj, Maddie Masinsin, and Elizabeth Sutterlin. Amelia Larson, David Meijer, Shannon O'Toole, Tyler Roylance, and Lora Uhlig edited the report.

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

This booklet is a summary of findings for the 2024 edition of *Freedom on the Net*. Narrative reports on 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 14th consecutive year. Protections for human rights online diminished in 27 of the 72 countries covered by *Freedom on the Net* (FOTN), with 18 earning improvements. Kyrgyzstan received this year's sharpest downgrade, as President Sadyr Japarov intensified his efforts to silence digital media and suppress online organizing. China shared its designation as the world's worst environment for internet freedom with Myanmar, where the military regime imposed a new censorship system that ratcheted up restrictions on virtual private networks (VPNs). At the other end of the spectrum, Iceland maintained its status as the freest online environment, and Zambia secured the largest score improvement. For the first time in 2024, FOTN assessed conditions in Chile and the Netherlands, both of which showcased strong safeguards for human rights online.

2

Free expression online was imperiled by severe prison terms and escalating violence. In three-quarters of the countries covered by FOTN, internet users faced arrest for nonviolent expression, at times leading to draconian prison sentences exceeding 10 years. People were physically attacked or killed in retaliation for their online activities in a record high of at least 43 countries. Internet shutdowns and reprisals for online speech created even more perilous environments for people affected by several major armed conflicts around the world.

3

Censorship and content manipulation were combined to sway elections, undermining voters' ability to make informed decisions, fully participate in the electoral process, and have their voices heard. Voters in at least 25 of the 41 FOTN countries that held or prepared for nationwide elections during the coverage period contended with a censored information space. In many countries, technical censorship was used to constrain the opposition's ability to reach voters, reduce access to reliable reporting, or quell concerns about voting irregularities. In at least 21 of the 41 countries, progovernment commentators manipulated online information, often stoking doubt about the integrity of the forthcoming results and seeding long-term mistrust in democratic institutions. In addition, interference from governments and a reduction in transparency mechanisms on major social media platforms chilled the efforts of independent researchers and media groups to shed light on election-related influence operations.

4

In more than half of the FOTN countries that held or prepared for elections, governments took steps aimed at addressing information integrity, with mixed results for human rights online. The interventions included enforcing rules related to online content, supporting fact-checking and digital literacy initiatives, and passing new guidelines to limit the use of generative artificial intelligence (AI) in campaigning. The impact on internet freedom depended on the extent to which each effort prioritized transparency, civil society expertise, democratic oversight, and international human rights standards. Examples from South Africa, Taiwan, and the European Union served as the most promising models.

5

Building a trustworthy online environment requires a renewed and sustained commitment to internet freedom. This year, FOTN indicators assessing limits on content dropped to their lowest average score in more than a decade, excluding the two countries covered in this edition for the first time—an indication that online censorship and manipulation are growing ever more extreme. The lack of access to a high-quality, reliable, and diverse information space has impeded people's ability to form and express their views, engage productively in their communities, and advocate for government and company accountability. Policy interventions designed to protect information integrity can help build confidence in the online environment, provided they are anchored in free expression and other fundamental rights. Responses that fail to incorporate those principles will only hasten the global decline in internet freedom and democracy more broadly.

Freedom on the Net 2024: The Struggle for Trust Online

By Allie Funk, Kian Vesteinsson, and Grant Baker

A rapid series of consequential elections have reshaped the global information environment over the past year. Technical censorship curbed many opposition parties' ability to reach supporters and suppressed access to independent reporting about the electoral process. False claims of voter fraud and a rise in harassment of election administrators threatened public confidence in the integrity of balloting procedures. Partisan efforts to delegitimize independent fact-checkers and researchers chilled their essential work. As a result, more than a billion voters had to make major decisions about their future while navigating a censored, distorted, and unreliable information space.

These trends contributed to the 14th consecutive year of decline in global internet freedom. Of the 72 countries covered by *Freedom on the Net 2024*, conditions for human rights online deteriorated in 27, and 18 countries registered overall gains. The year's largest decline occurred in Kyrgyzstan, followed by Azerbaijan, Belarus, Iraq, and Zimbabwe. Conversely, Zambia earned the largest improvement, as space for online activism opened. In more than three-fourths of the countries covered by the project, people faced arrest for expressing their political, social, and religious views online, while people were met with physical violence related to their online activities in a record high of at least 43 countries.

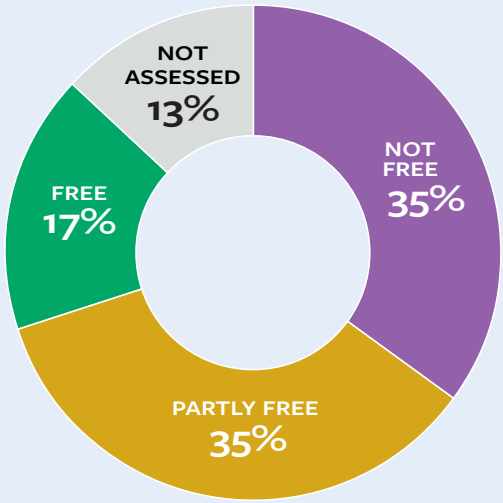
Wiping out online dissent

For the first time in 10 years, China shared its designation as the world's worst environment for internet freedom with a second country: Myanmar. Conditions there deteriorated to their lowest point in the history of FOTN. Since seizing power in a 2021 coup, Myanmar's military has conducted a brutally violent crackdown on dissent and imprisoned thousands of people in retaliation for their online speech, all while building a mass censorship and surveillance regime to suppress the activities of civilian prodemocracy activists and armed resistance groups. In May 2024, the military introduced new censorship technology to block most VPNs, cutting residents off from tools they had relied on to safely and securely bypass internet controls. At the same time, Beijing has persisted in its effort to isolate China's domestic internet from the rest of the world, blocking international traffic to some government websites and imposing huge fines on people using VPNs. The Chinese government also continued to systematically repress dissent, for example by censoring online discussion about activist and journalist Sun Lin, who died in November 2023 after police beat him in apparent retaliation for his social media posts about protests against Chinese Communist Party (CCP) leader Xi Jinping.

Well beyond the world's worst environments, many people faced harsh repercussions for expressing themselves online.

GLOBAL INTERNET POPULATION BY 2024 FOTN STATUS

Freedom on the Net assesses 86.7 percent of the world's internet user population.



GLOBAL INTERNET USER STATS

Over **5 billion** people have access to the internet.

According to Freedom House estimates:

79% live in countries where individuals were arrested or imprisoned for posting content on political, social, or religious issues.

67% live in countries where individuals have been attacked or killed for their online activities since June 2023.

66% live in countries where authorities deployed progovernment commentators to manipulate online discussions.

65% live in countries where websites hosting political, social, or religious content were blocked.

52% live in countries where access to social media platforms was temporarily or permanently restricted.

48% live in countries where authorities disconnected internet or mobile networks, often for political reasons.

In at least 56 of the 72 countries covered by FOTN, internet users were arrested due to their political, social, or religious expression. A Thai prodemocracy activist was sentenced to 25 years in prison in March 2024, having been convicted under the country's repressive lèse-majesté law for 18 posts about the monarchy on the social media platform X. Cuban authorities sentenced a woman to 15 years in prison for sedition and "enemy propaganda" after she shared images of protests on social media, including a video recording of police attacking demonstrators. In Pakistan, a court sentenced a 22-year-old student to death on blasphemy charges for preparing pictures and videos that denigrated the prophet Muhammad, and sentenced a 17-year-old to life in prison for sharing them on WhatsApp.

Authorities around the world limited access to online spaces that people used to consume news, connect with loved ones, and mobilize for political and social change. Governments in at least 41 countries blocked websites that hosted political, social, and religious speech during the report's June 2023 to May 2024 coverage period. In Kyrgyzstan, the government blocked the website of the independent media outlet Kloop after it reported on an imprisoned opposition figure's allegations of torture in detention. Authorities later ordered a full liquidation of the umbrella organization that runs the outlet, further reducing people's access to investigative reporting on government corruption and rights abuses. In at least 25 countries, governments restricted access to entire social media and communication platforms. French authorities ordered the blocking of TikTok in the French Pacific territory of New Caledonia to curb protests by members of the Kanak community, the island's Indigenous people, that grew violent in May 2024 amid dissatisfaction with proposed electoral reforms.

Internet freedom under fire

Retaliatory violence for online expression from both state and nonstate actors, as well as deteriorating conditions

> For the first time in 10 years, China shared its designation as the world's worst environment for internet freedom with a second country: Myanmar.

Palestinian journalists in the Gaza Strip attempt to connect to the internet. Armed conflicts around the world were made even more dangerous by restrictions on connectivity. (*Photo credit: Said Khatib/AFP/Getty Images*)

during armed conflicts, drove several score declines during the coverage period. In a record 43 countries, people were physically attacked or killed in reprisal for their online activities. In Iraq, where journalists, activists, and bloggers face routine violence, kidnappings, and even assassinations in retaliation for online speech, a prominent civil society activist was murdered in October 2023 by an unknown assailant after his Facebook posts encouraged Iraqis to engage in protests. A Belarusian online journalist reported being tortured by authorities in December due to his connection to one of the hundreds of independent news outlets that the government deems "extremist."

Armed conflicts were made even more dangerous by a lack of access to information and essential services. Internet shutdowns during fighting in Sudan, Ethiopia, Myanmar, the Gaza Strip, and Nagorno-Karabakh plunged people into information vacuums, prevented journalists from sharing reports about human rights abuses, and hampered the provision of desperately needed humanitarian aid. Amid the civil war in Sudan between the paramilitary Rapid Support Forces (RSF) and the regular Sudanese Armed Forces (SAF), the RSF captured internet service providers' data centers in Khartoum and cut off internet access across the country in February. The shutdown disrupted humanitarian groups' ability to deliver food, medicine, and medical equipment.

Forces vying for control during wartime also retaliated directly against people who reported on or discussed the conflicts online. Both the RSF and the SAF in Sudan tortured journalists and other civilians in response to perceived

About this report: This is the 14th edition of *Freedom on the Net*, an annual study of human rights online. The project assesses internet freedom in 72 countries, accounting for 87 percent of the world's internet users. FOTN 2024 assessed Chile and the Netherlands for the first time. Both serve as global models for internet freedom, with Chile ranking third—tied with Canada—and the Netherlands ranking sixth. This report covers developments between June 2023 and May 2024. More than 95 analysts and advisers contributed to this year's edition, using a standard methodology to determine each country's internet freedom score on a 100-point scale, with 21 separate indicators pertaining to obstacles to access, limits on content, and violations of user rights. The FOTN website features in-depth reports and data on each country's conditions.

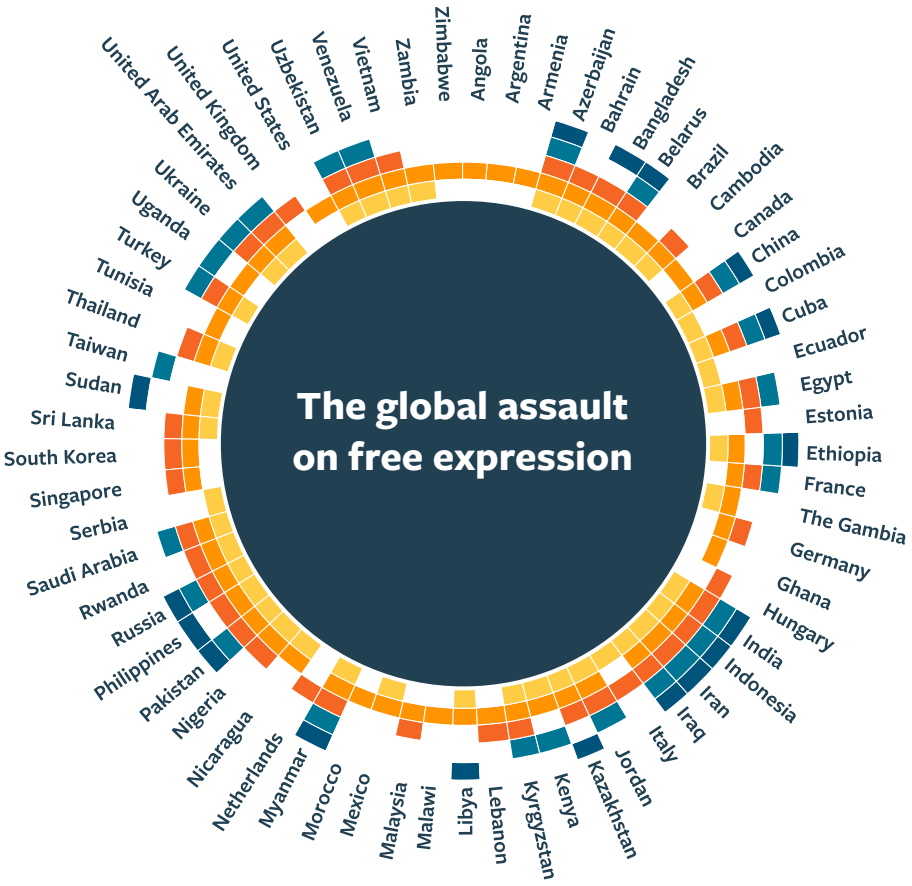
criticism on digital platforms. During the Azerbaijani military's offensive in Nagorno-Karabakh in September 2023, authorities in Baku detained several people for a month, including former diplomat Eman Ibrahimov, because of social media posts that criticized the operation or called for a peaceful resolution of the conflict.

The impact of the devastating war between Israel and the militant group Hamas reverberated around the world. (Israel and the Israeli-occupied Palestinian territories are not among the 72 countries covered by FOTN.) People in several countries, including Bahrain, Saudi Arabia, and Singapore, faced repercussions for expressing their views about the conflict online. In Jordan, dozens of users were arrested between October and November 2023 under the country's repressive new cybercrime law for their posts criticizing the Jordanian government's relationship with Israel or calling for protests in support of the Palestinian cause. More broadly, independent researchers documented a surge of antisemitic and anti-Muslim hate speech online, a proliferation of false and misleading content about the conflict, and an increase in disproportionate restrictions on pro-Palestinian and other Palestine-related content by Facebook's and Instagram's moderation systems.

> Forces vying for control during wartime retaliated directly against people who reported on or discussed the conflicts online.

Elections focus attention on a trust deficit in the information space

In 2024, FOTN's indicators assessing limits on content—including website blocking, disproportionate content removal, censorship laws, self-censorship practices, content manipulation, and constraints on information



Extreme censorship, arrests, and rising violence against people imperiled internet freedom around the world.

- Internet connectivity deliberately disrupted
- Social media or communications platforms blocked
- Websites hosting political, social, or religious content blocked
- Internet user arrested or imprisoned for online activities
- Internet user physically attacked or killed for online activities

diversity—dropped to their lowest average score in more than 10 years, excluding the two countries that were covered for the first time in this edition. Today's information space contributes to and is degraded by many of the same challenges affecting human society more broadly: rising political polarization, a chilling of civic participation, partisan efforts to undermine confidence in elections, and a long-term erosion of trust in democratic institutions. These problems have interfered with people's fundamental rights to seek, receive, and impart diverse information, form opinions, and express themselves online.

Today's information space contributes to and is degraded by many of the same challenges affecting human society more broadly.

As voters around the world headed to the polls in 2024, the preexisting threats to the information space only grew more acute. Freedom House and other commentators had warned that a perfect storm of challenges could prove disastrous for information integrity during the year. Generative AI has become more accessible, lowering the barrier of entry for those seeking to create false and misleading information. Many social media companies have laid off the very teams that were dedicated to advancing trust, safety, and human rights online. These warning signs served as a catalyst for efforts aimed at rebuilding confidence in online information during the coverage period. Policymakers, tech companies, and civil society groups experimented with ways to strengthen platform governance, boost digital literacy, and incentivize more responsible online behavior. Some initiatives showed promise, though it is still too early to assess their efficacy. Others failed to adequately protect internet freedom while attempting to address false, misleading, and incendiary content. To foster an online environment that offers high-quality, diverse, and trustworthy information, successful policies must include robust protections for free expression and other fundamental rights.

Controlling information to tilt an election

Many governments sought to control electoral outcomes while still claiming the political legitimacy that only a free and fair election can confer. Their curation of the online information space through censorship and content manipulation often reinforced offline efforts to plant seeds of doubt in or rig the voting itself. For example, a number of incumbents restricted access to content about the opposition, reducing their opponents' ability to persuade and mobilize voters, or simply boosted their own preferred narratives about the election results. Censorship and content manipulation frequently began well before an electoral period, disrupting the crucial discussion and debate necessary for voters to form and express their views.

Obstruction of access to diverse information

In 25 of the 41 FOTN countries that held or prepared for nationwide elections during the coverage period, governments blocked websites hosting political, social, and religious speech; restricted access to social media platforms; or cut off internet connectivity altogether. Blocking websites, the most common form of election-related censorship, allowed authorities to selectively restrict content that they deemed objectionable, such as reporting on corruption or evidence of voting irregularities, while maintaining access to information that worked in their favor. Internet shutdowns were the least common election-related censorship tactic, suggesting that authorities are more reluctant to impose such extreme and unpopular restrictions during balloting. When they did occur, shutdowns were most often aimed at reducing opposition parties' ability to communicate with voters ahead of an election or to quash postelection protests over alleged fraud.

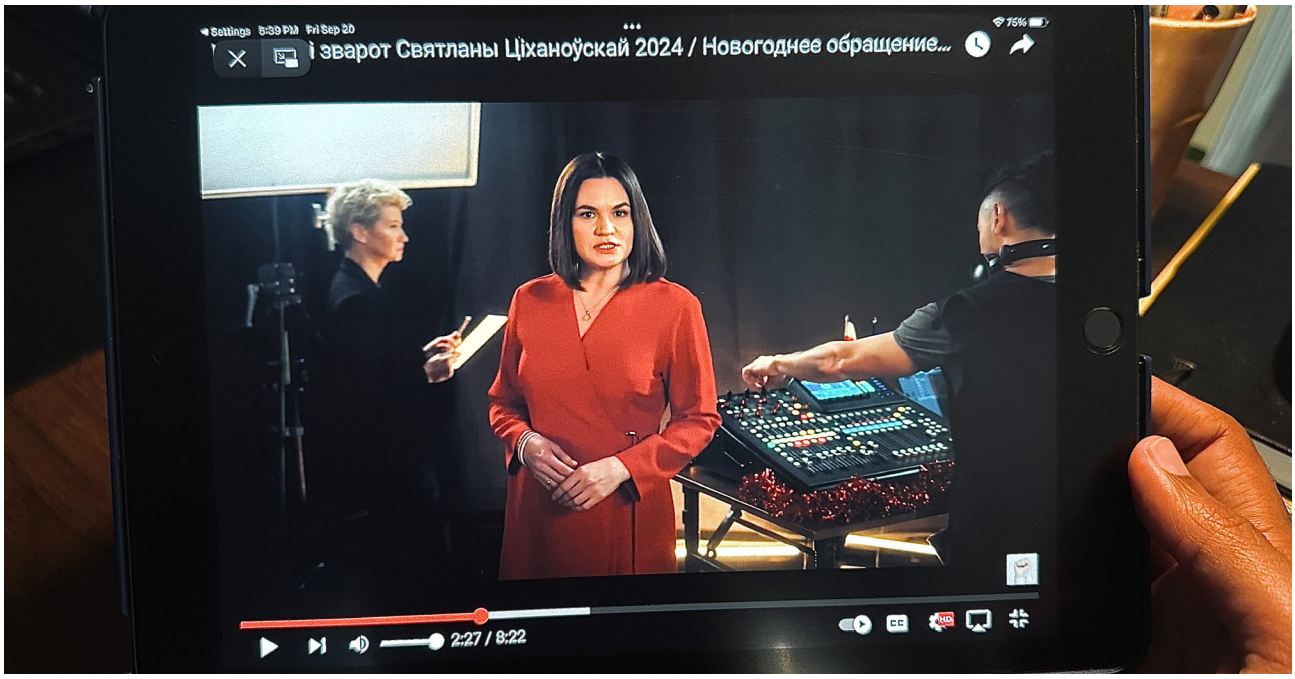
Technical censorship limits independent information and reduces electoral competition

Technical censorship was often used to suppress access to independent reporting, criticism of the government, and civil society websites, mirroring a given state's broader offline restrictions over news media. Officials in Cambodia ordered internet service providers to block access to independent news websites a week before the July 2023 elections, further tightening media controls during a balloting process that was thoroughly engineered to suppress challenges to the ruling Cambodian People's Party.

Governments also deployed technical censorship to stymie the opposition's ability to engage with voters. Ahead of Bangladesh's January 2024 elections, authorities temporarily restricted internet connectivity when the main opposition Bangladesh Nationalist Party (BNP) held a large rally in October 2023, limiting online discussion of the event and impeding the party's digital outreach to supporters. In the run-up to Belarus's openly rigged parliamentary elections, in February 2024, officials partially restricted access to YouTube to prevent Belarusians from watching exiled opposition leader Sviatlana Tsikhanouskaya's New Year address. To mock the government's own information controls, however, the Belarusian opposition created Yas Gaspadar, a made-up candidate generated by AI, claiming that he could speak freely to voters online without risking arrest.

Repressive regimes that faced strong opposition challengers resorted to the most brazen forms of censorship in their bids to maintain power. During Pakistan's February 2024 general elections, the military used harsh offline methods to suppress support for former prime minister Imran Khan and his Pakistan Tehreek-e-Insaf (PTI) party, imprisoning Khan and other party leaders, barring Khan from running, and forcing

Repressive regimes that faced strong opposition challengers resorted to the most brazen forms of censorship in their bids to maintain power.



Authorities in Belarus restricted access to YouTube in an attempt to prevent people from watching opposition leader Sviatlana Tsikhanouskaya deliver a speech ahead of the 2024 elections. (*Photo credit: Freedom House*)

the PTI to field its candidates as independents. To bypass the crackdown, the PTI organized virtual rallies and deployed a generative AI avatar of Khan to deliver speeches that he wrote behind bars. The military intensified its censorship in response, with users reporting difficulty accessing the internet and social media platforms during the virtual rallies. On election day, authorities restricted mobile connectivity, and some voters stated that the restrictions limited their ability to locate polling stations. After the vote, as results showed a strong performance by PTI-linked candidates and the party's supporters gathered on X to allege voting irregularities, authorities blocked the platform, as well as websites created by the party to document purported vote rigging.

In Venezuela, ahead of an independently organized opposition primary in October 2023, the authoritarian regime of Nicolás Maduro ordered the blocking of sites that allowed voters to locate polling stations. The move aligned with Maduro's offline interference, including a ruling by the politicized Supreme Tribunal of Justice that barred the primary's winner, María Corina Machado, from running in the July presidential election, held after FOTN's coverage period. In July, when vote tallies collected by the opposition showed that Maduro had been soundly defeated by a Machado ally, former diplomat Edmundo González Urrutia, the regime ratcheted up its censorship apparatus to support Maduro's claims of victory. Authorities blocked Signal, X, and a host of media and civil society websites as part of their drive to quell mass protests, cut the opposition leadership off from its supporters, and reduce access to independent news about the election results and the state's offline crackdown.

Censorship laws threaten electoral speech

Authorities in many countries enacted stricter laws and regulations governing online content, effectively deterring people from reporting on elections and expressing their views about candidates and policies. Ahead of an early presidential election in June and July, authorities in Iran—the world's third most repressive internet freedom environment—criminalized any content that encouraged election boycotts or protests, or that criticized candidates. The rules were, at least in part, aimed at garnering higher voter turnout to make the election seem legitimate, despite the arbitrary disqualification of most candidates. Iran's judiciary also warned that the electoral law prohibited candidates and their supporters from using foreign social media platforms, almost all of which are blocked in the country.

In the run-up to Russia's sham March 2024 presidential election, the Kremlin enacted a slew of laws that further

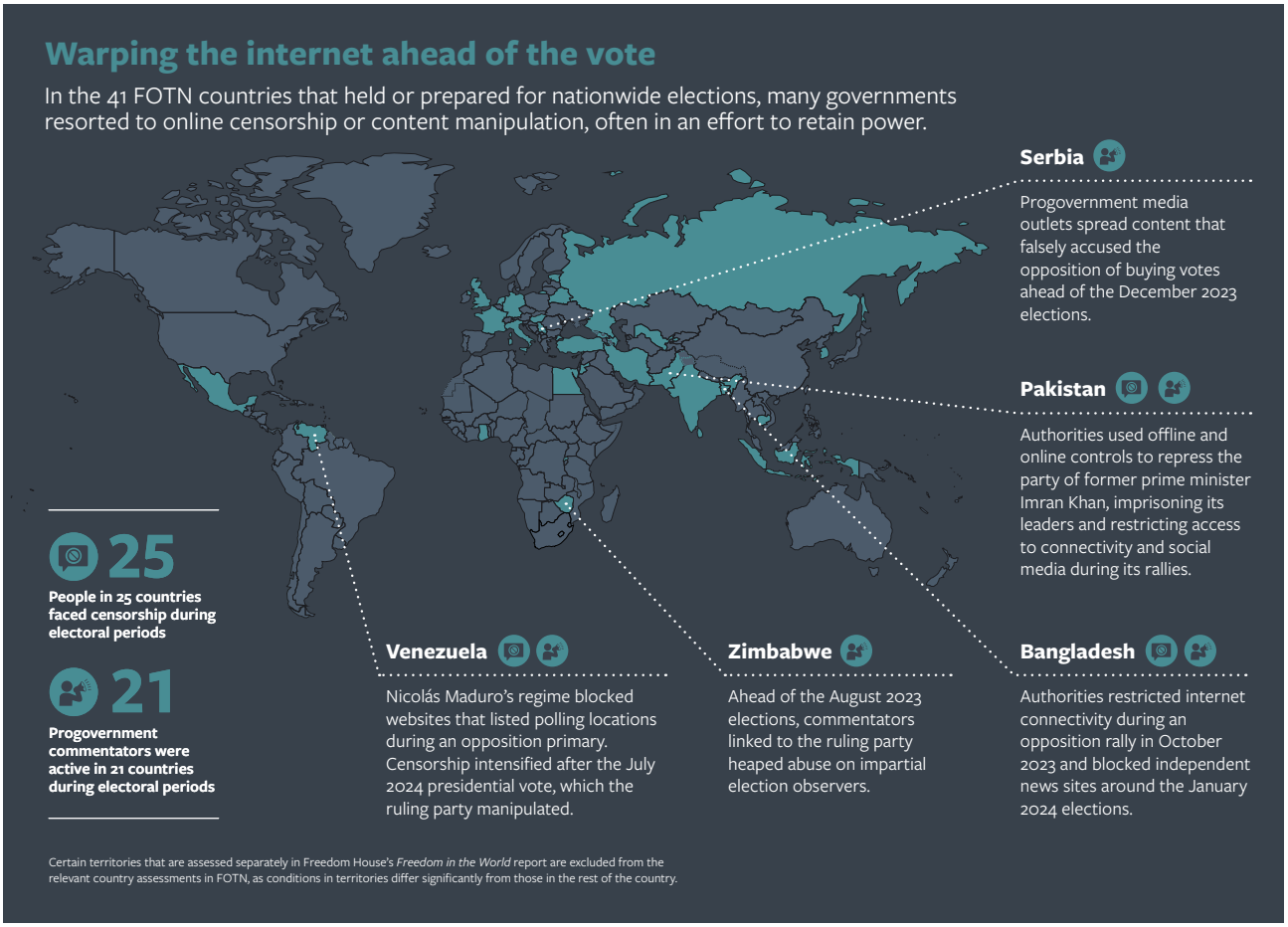
smothered what was already a heavily restricted information environment. One law criminalized the advertisement of VPNs, advancing the government's existing efforts to limit the use of such tools to access uncensored information. A February 2024 law banned Russians from advertising on websites and social media channels that were labeled as "foreign agents," forcing the country's few remaining independent media channels, largely active on Telegram and YouTube, to downsize their operations and lay off staff.

Distortion of the information space

Progovernment commentators who used deceitful or covert tactics to manipulate online information were active in at least 21 of the 41 FOTN countries that held or prepared for nationwide elections during the coverage period. Content manipulation campaigns warped online discussion by perpetuating falsehoods about the democratic process, manufacturing inauthentic support for official narratives, or discrediting those who presented a threat to the leadership's political dominance. These networks often worked in tandem with state-controlled or -aligned news media, deployed bot accounts across social media, generated fake websites to spoof real news outlets, and harnessed genuine enthusiasm from political loyalists. Such content manipulation is a less visible form of control than outright censorship, and it may trigger less political blowback, making it a lower-risk tactic that can yield the high reward of reshaping an online environment and even winning an election.

An evolution of players and tactics

The actors involved in disinformation campaigns, as well as their incentives and the technology they employ, have evolved in recent years. To gain plausible deniability regarding their involvement, political leaders have increasingly outsourced content manipulation to social media influencers and shady public-relations firms that benefit from lucrative contracts or political connections. Influencers who participate in content manipulation leverage the trust and loyalty they have built with their followers to promote false, misleading, or divisive



messages. In Taiwan, for example, fashion and makeup influencers posted false claims about vote rigging ahead of the country's January 2024 elections. The claims mirrored an influence campaign originating in China that aimed to discourage voting in Taiwan.

The purveyors of false and misleading information have adapted to a proliferation of platforms and their varying policies and practices on content moderation. As a given narrative pinballs across different video-, image-, and text-based applications, mitigation measures carried out by any single company have less effect. Companies that have grown their user base significantly in recent years, such as Twitch, are playing catch-up when it comes to countering false and misleading information at scale. Others, like Telegram, have become breeding grounds for such campaigns because of their explicitly hands-off approach to content moderation. Research has also pointed to a rise in false, misleading, and hateful content on X after the company drastically relaxed its approach to content moderation, cut staffing on a number of teams, and introduced other concerning policies.

Freedom on the Net 2023 documented the early adoption of generative AI as a means of distorting narratives on political and social topics. During this coverage period, generative AI was frequently used to create false and misleading content. Ahead of Rwanda's July 2024 elections, a network of accounts spread AI-generated messages and images in support of incumbent president Paul Kagame. Chatbot models offered by major tech companies also spewed inaccurate or partially accurate information about registering to vote, voting by mail, or other procedures in several elections, demonstrating how poorly they are equipped to provide high-quality election information.

However, generative AI does not yet seem to have dramatically enhanced the impact of influence operations. Available evidence from civil society, academia, and media investigations suggests that generative AI–assisted disinformation campaigns have had a minimal impact on electoral outcomes. OpenAI reported in May that the company had disrupted attempts by actors linked to China, Iran, Israel, and Russia to use ChatGPT as a component in more conventional influence campaigns, which failed to generate much reach or engagement. It takes time for governments and those they employ to effectively incorporate new techniques into influence operations, and generative AI is just one of many tools at their disposal. There is also a major research gap in terms of detecting these campaigns in general and identifying their use of generative AI specifically, limiting public knowledge on the impact of the technology.

> Content manipulation campaigns attempted to delegitimize electoral institutions, intimidate election officials, or falsely claim that electoral processes were rigged in the opposition's favor.

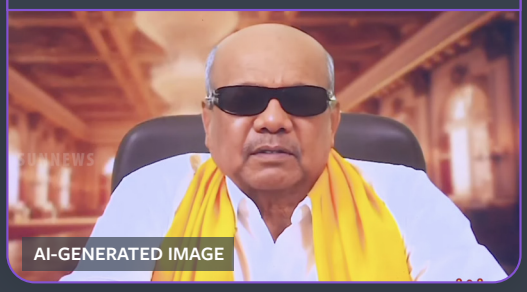
Sowing doubt in the integrity of elections

Disinformation campaigns during the coverage period commonly broadcast false and misleading narratives that painted electoral institutions and processes as rigged, alleged foreign interference, or in the most authoritarian states, claimed that a fraudulent election was legitimate. While such campaigns are partisan by definition, their effect extends beyond a particular candidate or party, causing voters to distrust the outcome of the balloting itself. Left unchecked, they seed long-lasting skepticism or even cynicism about elections and can undermine public trust in democratic institutions over time.

Several campaigns over the past year attempted to delegitimize electoral institutions, intimidate election officials, or falsely claim that electoral processes were rigged in the opposition's favor. In Zimbabwe, supporters of the ruling party harassed independent election observers during the August 2023 elections, maligning them as biased against the government. Ahead of Serbia's December 2023 elections, progovernment tabloids published false and misleading information about the opposition and independent media, including a fake video purporting to show the political opposition buying votes. These campaigns disproportionately target women who play a prominent role in political processes. In South Africa, a fusillade of online attacks was directed at electoral commission member Janet Love, with many accusing her of rigging the vote; the attacks largely came from supporters of Jacob Zuma, a former president who sought to delegitimize the commission as part of his effort to stage a political comeback in the May 2024 elections.

Narratives asserting that politicians were influenced by foreign interests were also common. Fueled in part by

India



A political party in Tamil Nadu circulated AI-generated videos of its long-dead founder to mobilize its activists.

Rwanda

A progovernment network used AI image-generation tools to mock critics of the ruling party, though the posts had little reach or engagement.

Indonesia

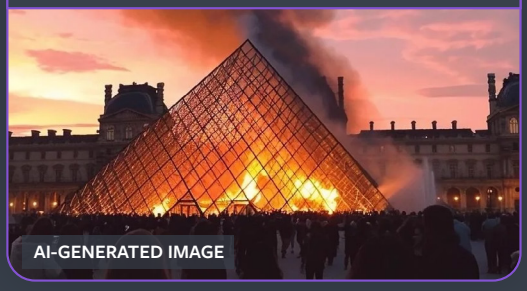
President-elect Prabowo Subianto used an AI-generated avatar to rebrand himself as "cuddly," papering over credible allegations that he had committed rights abuses as a military commander.

Generative AI at the ballot box

Belarus

The opposition created Yas Gaspadar, a made-up candidate with an AI-generated avatar, to mock the government's censorship regime.

European Union



Maldita.es, a fact-checking group within the European Digital Media Observatory network, debunked an AI-generated photo that spread a rumor that immigrants had set the Louvre on fire.

Pakistan

When former prime minister Imran Khan was jailed ahead of the election, his party deployed a generative AI avatar to deliver speeches that he wrote behind bars.

comments from officials of the then-ruling Awami League about foreign pressure on the elections, progovernment Bangladeshi bloggers painted the opposition BNP as a tool of US interests. In the lead-up to the June 2024 European Parliament elections, influencers who support Hungary's ruling Fidesz party published videos characterizing the Hungarian political opposition as the "dollar left" and independent news outlets as the "dollar media," implying that they do the bidding of foreign donors.

In authoritarian countries, progovernment commentators mobilized to depict sham elections as free and fair. Azerbaijan's regime enlisted content creators from around the world—compensated with free travel and accommodation in Baku—to acclaim the integrity of the February 2024 elections, which were heavily manipulated to favor incumbent president Ilham Aliyev. The efforts built on Azerbaijani officials' long-running attempts to legitimize their rigged elections, including the funding of ersatz election-observation missions.

In authoritarian countries, progovernment commentators mobilized to depict sham elections as free and fair.

Attempts to delegitimize fact-checkers

Government actors in several countries launched direct attacks—in the form of disinformation campaigns, online harassment, or other forms of political interference—on the work of independent researchers and fact-checkers who are dedicated to unmasking influence operations and boosting trustworthy information. As a result, some initiatives were forced to shutter or reduce their operations, leaving voters in the dark about attempts to spread false information and undermining societal resilience in the face of electoral manipulation. Governments also established more friendly alternatives to independent fact-checkers, seeking to harness the trusted practice of fact-checking for their own political benefit.

In some of the most repressive environments, governments have long worked to delegitimize or co-opt fact-checking. On the day of Egypt's December 2023 presidential election, the country's media authority launched an investigation into the fact-checking platform Saheeh Masr. The site had reported that the state-owned conglomerate United Media Services ordered affiliated outlets to suppress election reporting, including stories that showed low turnout or voters facing pressure to choose a particular candidate.

Democracies were not immune to this trend during the coverage period. Weeks before balloting began in India's general elections, the central government sought to stand up a fact-checking unit that would "correct" purportedly false reporting on official business. Indian journalists and civil society groups criticized the project as ripe for abuse, and the country's highest court temporarily paused the creation of the unit. Similarly, the *Washington Post* reported that an Indian disinformation research hub was in fact linked to the national intelligence services, finding that it laundered talking points in support of the ruling Bharatiya Janata Party (BJP) alongside fact-based research.

South Korean president Yoon Suk-yeol and his People Power Party employed the rhetoric of "fake news" to justify a campaign against independent media ahead of April 2024 legislative elections. Authorities raided and blacklisted independent media outlets that had reported critically on the government, and People Power Party legislators launched a campaign to tar South Korea's primary fact-checking platform, the nonprofit SNUFactCheck, as biased. The accusations reportedly caused a major sponsor to withdraw funding from SNUFactCheck, which had operated through a partnership between Seoul National University and dozens of prominent media outlets. The funding crisis led the center to suspend activities indefinitely as of August 2024, depriving residents of a crucial service that helped them distinguish fact from fiction online.

Similar pressure on independent experts in the United States has left people less informed about influence operations ahead of the November elections. A coalition of researchers known as the Election Integrity Partnership (EIP), which had conducted analysis of—and at times notified social media companies about—false electoral information during the 2020 campaign period, faced intense pressure and scrutiny. False allegations about the EIP's work, including that it fueled government censorship, prompted a wave of litigation, subpoenas from top Republicans on the US House of Representatives' Judiciary Committee, and online harassment aimed at EIP participants. This concerning campaign has raised the cost of working on

information integrity and produced a chilling effect in the broader community of US experts on the topic. Individual experts and institutions have reported scaling down their activities and limiting public discussion of their work to avoid similar hostility or hefty legal fees.

Companies also reduced access to data about activities on their platforms, hampering the ability of fact-checkers and independent researchers to study the information space. In August 2024, Meta shut down CrowdTangle, a critical tool that allowed real-time analysis of content across Facebook and Instagram, and replaced it with a far more limited alternative. In September 2023, X banned nearly all scraping on its site, cutting off a primary source of data for researchers. The move built on an earlier change that locked access to X's interface for researchers behind an exorbitantly expensive paywall. Researchers' access to platform data allows them to uncover harassment and disinformation campaigns, unmask the actors behind them, and flag key trends on social media. Limiting access to this information makes it more difficult to design effective policies and technical interventions for strengthening internet freedom.

> Pressure on independent experts in the United States has left people less informed about influence operations ahead of the November elections.

Developing remedies that protect internet freedom

In more than half of the 41 FOTN countries that held or prepared for nationwide elections during the coverage period, governments took steps aimed at making the information space more reliable. Common interventions included engaging with technology companies to boost authoritative information from election commissions or to address false and misleading information; supporting fact-checking initiatives led by local media and civil society; and setting rules for how political campaigns can use generative AI. The measures often varied within a given country, with regulatory bodies taking different—and at times conflicting—approaches based on their mandate, legal authority, structural independence, and political incentives.

To determine whether these efforts strengthened or undermined internet freedom, Freedom House assessed them based on four criteria: transparency in their decision-making and related processes, meaningful engagement with local civil society, independent implementation and democratic oversight, and adherence to international human rights standards. These features, when present, helped guard against government overreach and company malfeasance, fostered trust and legitimacy with the public, allowed for open debate about how to address false and misleading content, and facilitated the incorporation of diverse expertise that leads to more informed and effective actions. The most promising approaches were found in South Africa, the European Union (EU), and Taiwan, whose interventions largely met all four criteria.

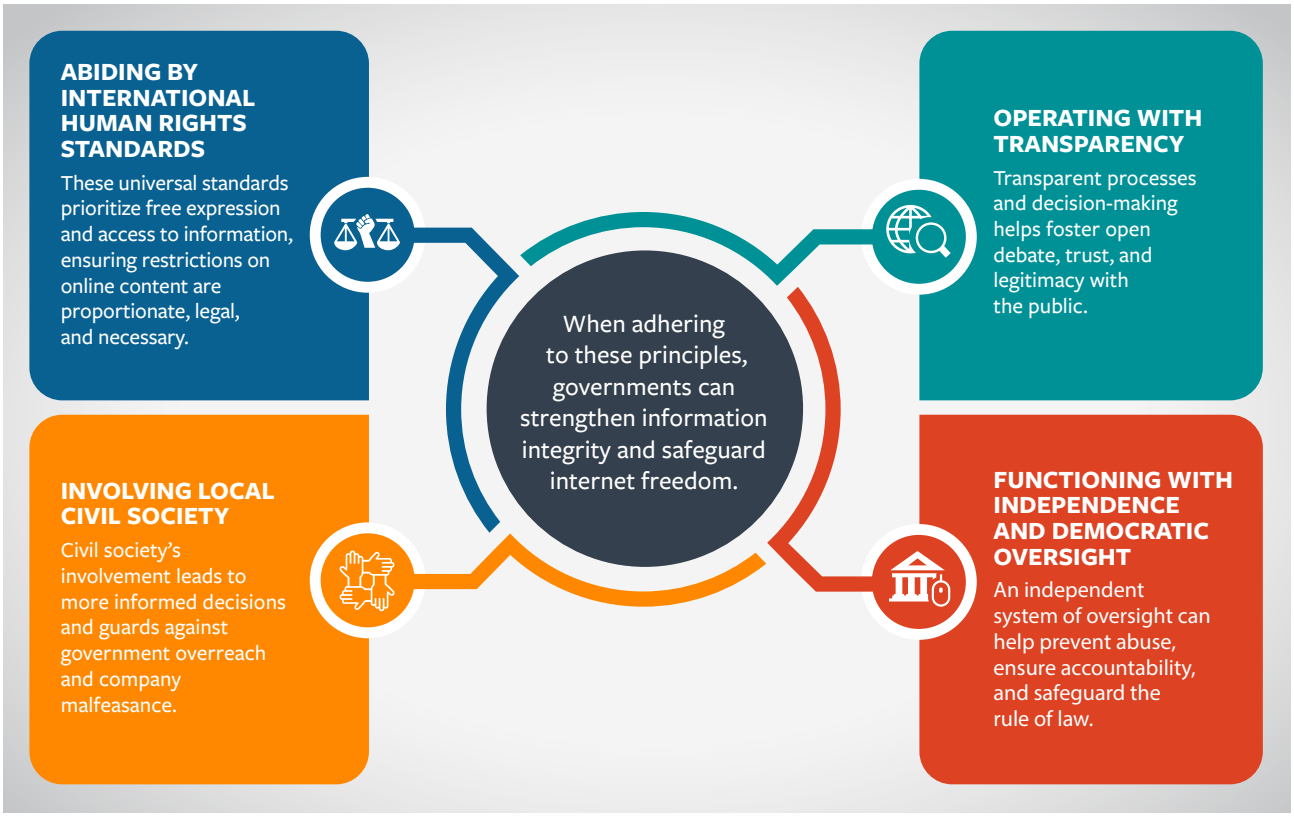
The efforts of Brazil's Superior Electoral Court demonstrated the complexity of upholding internet freedom while countering disinformation campaigns.

A myriad set of factors limited assessment of whether the actions explored in this report were effective at fostering a high-quality, diverse, and trustworthy information environment. For one, the utility of each remedy depended on each setting's unique context, such as a country's political dynamics or legal framework. The same fact-checking initiative that proves effective in an established democracy may flounder in an environment where the state exercises control over online media. Several policies were simply too new to assess, as countering false and misleading information is generally a long-term endeavor. The voluntary or nontransparent nature of many interventions also made enforcement difficult to track. Finally, research gaps, created in part by government pressure that has chilled the work of fact-checkers and by company decisions to roll back access to platform data, hamper understanding of how false, misleading, and incendiary content spreads and the extent to which interventions are addressing the problem.

When state regulators overstep

In the periods surrounding major elections, many governments attempted to address false, misleading, or incendiary content by enforcing content-removal rules among technology companies. The most problematic efforts lacked transparency and robust oversight, failed to involve civil society, and unduly restricted free expression and access to information. The risks of overreach were most profound in settings where some forms of protected online speech were already criminalized, the rule of law was weak, and regulatory bodies lacked independence.

Ahead of Indonesia's February 2024 elections, authorities launched efforts to address purportedly illegal content online, but the initiative was marred by opacity that raised concerns about abuse. The elections oversight agency Bawaslu, the communications regulator Kominfo, and the national police established a joint election desk to identify and request the removal of "illegal" content by platforms, in part reportedly due to frustrations that tech companies had failed to adequately



act on complaints during the 2019 elections. The likelihood of overreach was increased by the fact that decision-making was left in the hands of regulatory and law enforcement bodies, rather than an independent judiciary with a better record of protecting free expression. Kominfo has previously used the country's broad definitions of "illegal" speech to censor LGBT+ content, criticism of Islam, and expressions of support for self-determination in the Papua region.

In India, partisan officials forced tech companies to toe a favorable line ahead of the 2024 elections, displacing the more independent Election Commission of India (ECI) from its role overseeing election-related online information. The ECI declined to strengthen its Voluntary Code of Ethics, a 2019 agreement with platforms that sets out some brief but inadequate commitments regarding online content for the campaign period, and then enforced it sparingly and inconsistently. The ECI's soft touch created space for intervention by the far more politicized Ministry of Information and Broadcasting, which censored BJP critics, independent media, and opposition activists during the campaign. For example, pursuant to orders from the ministry in early 2024, X and Instagram restricted India-based users from viewing accounts that had mobilized as part of a farmers' protest movement to advocate for a stronger social safety net.

As Brazil prepared for countrywide municipal elections in October 2024, the efforts of the Superior Electoral Court (TSE) to safeguard election integrity demonstrated the complexity of upholding internet freedom while countering disinformation campaigns. In February, the TSE issued new rules requiring social media platforms to immediately remove posts that could undermine election integrity if they are "notoriously false," "seriously out of context," or present "immediate threats of violence or incitement" against election officials. Platforms that fail to comply face escalating civil penalties. Such problematic content can reduce people's access to reliable voting information, chill the work of election administrators, and contribute to offline violence. However, the guidelines' vague categorization and tight removal deadlines risk incentivizing excessive content removal, potentially affecting speech that should be protected under international human rights standards. Greater transparency from the TSE on its legal justification for content restrictions and associated orders to companies would provide much-needed insight into these rules' impact

on free expression and allow civil society to hold the TSE accountable when it oversteps.

In addition, Brazil's Supreme Court has pursued clearly disproportionate restrictions on free expression in a parallel effort to address false, misleading, and incendiary content that has contributed to offline violence in the country. Supreme Court justice Alexandre de Moraes, who led the TSE from August 2022 to June 2024, ordered the blocking of X in August 2024, after the coverage period, as part of a months-long dispute over the platform's refusal to comply with court orders restricting far-right accounts that were accused of spreading false and misleading information. The blocking order, which severed millions of Brazilians from the platform and was upheld by a panel of Supreme Court justices in early September, also concerningly threatened fines for people using anticensorship tools like VPNs to access X. The dispute between Moraes and X escalated into displays of brinksmanship in which X owner Elon Musk launched invectives and insults at the justice and flouted rules requiring foreign companies to have a local presence, while Moraes extended his enforcement efforts to Starlink and its parent company SpaceX, of which Musk is the chief executive and largest shareholder.

A more rights-respecting way to address problematic content

Some countries have developed more promising efforts to deal with false, misleading, or incendiary content, emphasizing transparency, the involvement of local civil society, democratic oversight, and adherence to international human rights standards.

South Africa's approach surrounding its May 2024 elections is one such positive example. The Real411 portal, led by the Electoral Commission of South Africa (IEC) and the civil society group Media Monitoring Africa (MMA), allowed the public to report cases of false information, harassment, hate speech, and incitement to violence, which were then assessed by media, legal, and technology experts to determine whether they met a set of narrow definitions for each category of content. If they did, the IEC could refer the content to the Electoral Court to determine whether it violated election laws, to platforms to determine whether it violated their terms of service, or to the media to raise awareness about or debunk false narratives. The IEC and MMA also created Padre, an online repository designed to catalog and increase transparency regarding political parties' spending on and placement of political advertisements. Independent experts' involvement in the IEC's initiatives helped ensure that decisions about online content were proportionate, specific, and protective of free expression.

A view of the election results announcement hosted by the Electoral Commission of South Africa, which worked with civil society groups to address problematic online content during the May 2024 elections. (*Photo credit: Michele Spatari/AFP/Getty Images*)

South African civil society served as a bulwark against another regulator's more disproportionate efforts to mitigate electoral misinformation. Proposed rules from the Film and Publication Board, which were withdrawn after civil society challenged their constitutionality, would have required companies to restrict access to vaguely defined "misinformation, disinformation, and fake news," and imposed criminal penalties—including prison terms of up to two years—for people who spread allegedly prohibited content.

Ahead of European Parliament elections in June, the EU used its unique market size and regulatory toolkit to compel social media platforms and search engines to increase transparency and mitigate electoral risks. The Digital Services Act (DSA), which entered into full force in February 2024, requires large platforms and search engines to provide detailed transparency reports, risk assessments, and researcher access to platform data, among other stipulations. In April 2024, the European Commission produced election guidelines that laid out the measures these companies should adopt under the DSA, such as labeling political ads and AI-generated content and ensuring that internal election-related teams were adequately resourced. Invoking the DSA, the commission opened formal proceedings against Meta and X for a host of possible violations, including Meta's suspected noncompliance on limiting deceptive electoral advertising and X's deficiencies in mitigating election-related risks.

The EU's nonobligatory Code of Practice on Disinformation served as a separate mechanism to strengthen information integrity. The code enlists signatories, including major platforms and advertising companies, to preemptively debunk and clearly label "digitally altered" content, set up transparency centers, and demonetize false and misleading information. These steps can help supply voters with the reliable information they need to make informed electoral decisions and fully participate in balloting. However, the voluntary nature of the code makes its effectiveness unclear and hard to track.

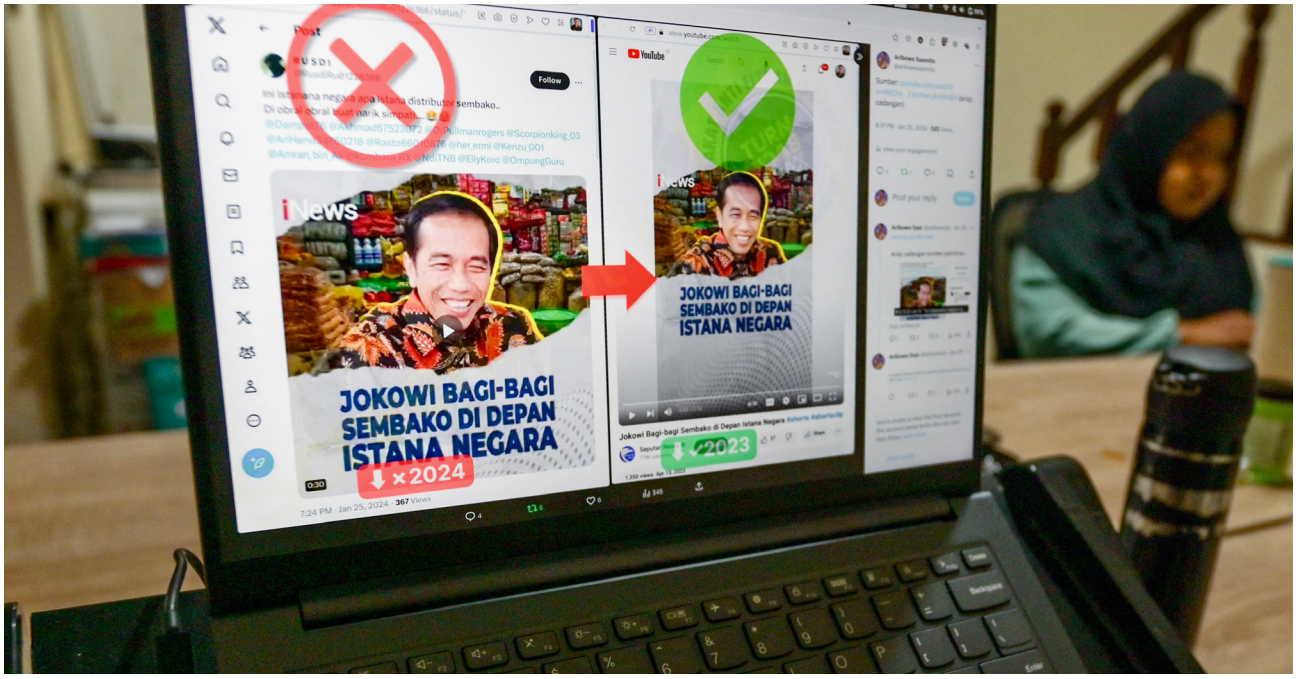
With robust oversight and safeguards for free expression, information sharing between democratic governments and tech companies can improve users' ability to access authoritative and reliable information. Government agencies may be privy to information about foreign actors, for example, that could provide context to companies as they seek to combat cyberattacks or coordinated inauthentic behavior. Federal agencies in the United States rolled back cooperation with platforms in a critical period leading up to the November 2024 elections, as they navigated legal challenges from state officials in Louisiana and Missouri. The two states, joined by private plaintiffs, had sued the federal government in 2022, claiming that its interactions with tech companies during the 2020 election period and the COVID-19 pandemic amounted to "censorship." The Supreme Court dismissed the case in June 2024, ruling that the plaintiffs did not prove harm and noting that a lower court's judgment in their favor had relied on "clearly erroneous" facts. The high court did not issue more detailed guidance on how agencies should communicate with platforms in alignment with constitutional free speech protections. As a result of the proceedings, the Federal Bureau of Investigation disclosed plans to increase transparency and set clearer guardrails around its engagement with platforms.

> Civil society's involvement in South Africa's initiatives helped ensure that decisions about online content were proportionate, specific, and protective of free expression.

Support for fact-checking and digital literacy

The coverage period featured several positive initiatives aimed at facilitating voters' access to authoritative information, such as through fact-checking programs, centralized hubs of resources, or digital literacy training.

Taiwan's civil society has established a transparent, decentralized, and collaborative approach to fact-checking and disinformation research that stands as a global model. Ahead of and during the country's January 2024 elections, these fact-checking programs helped build trust in online information across the political spectrum and among diverse constituencies. The Cofacts platform allowed people to submit claims they encountered on social media or messaging platforms for fact-checking by Cofacts contributors, who include both professional fact-checkers and nonprofessional community members. During the election period, Cofacts found that false narratives about Taiwan's foreign relations, particularly with the United States, were dominant on the messaging platform Line. Other local civil society organizations, such as IORG and Fake News Cleaner, also cultivated resistance to disinformation campaigns by



Indonesian fact-checkers worked to debunk false posts about the February 2024 elections. (*Photo credit: Bay Ismoyo/AFP/Getty Images*)

conducting direct outreach and programming in their communities.

Ahead of India's elections, more than 50 fact-checking groups and news publishers launched the Shakti Collective, the largest coalition of its kind in the country's history. The consortium worked to identify false information and deepfakes, translate fact-checks into India's many languages, and build broader capacity for fact-checking and detection of AI-generated content. The diversity of members in the Shakti Collective allowed it to reach varied communities of voters and identify emerging trends, such as an increase in false claims in regional languages that electronic voting machines were rigged.

> There remains a fundamental structural imbalance between fact-checkers and the purveyors of disinformation campaigns: it takes far more time and effort to prove that a claim is false than it does to create and spread it.

Governments in some countries supported the implementation of these sorts of programs. The independently run European Digital Media Observatory (EDMO), established in 2018 by the EU, conducted research and collaborated with fact-checking and media literacy organizations during the European Parliament election period. EDMO uncovered a Russia-linked influence network that was running fake websites in several EU languages, and also found that generative AI was used in only about 4 percent of the false and misleading narratives they detected in June. Mexico's National Electoral Institute (INE) launched Certeza INE 2024, a multidisciplinary project to counter electoral disinformation, ahead of the country's June elections. As part of the program, voters could ask questions about how to vote and report articles, imagery, and audio clips to "Ines," a virtual assistant on WhatsApp. Content flagged by voters would then be fact-checked through a partnership that included Meedan, Agence France-Press, Animal Político, and Telemundo.

Fact-checkers are often among the first to identify trends in false narratives, the actors responsible, and the technology they use. Their insights can inform effective policy, programmatic, and technological interventions that will advance internet freedom. However, while academic research has found fact-checking to be effective in certain contexts, it may not always lead to broader behavioral

shifts by users. There also remains a fundamental structural imbalance between fact-checkers and the purveyors of disinformation campaigns: it takes far more time and effort to prove that a claim is false than it does to create and spread it. These initiatives may face particular difficulties in highly polarized environments, as voters who already lack trust in independent media groups will be unlikely to believe their fact-checking work.

Regulations on generative AI in political campaigns

Spurred by concerns that generative AI would blur the line between fact and fiction during consequential voting, regulators in at least 11 of the 41 FOTN countries that held or prepared for nationwide elections during the coverage period issued new rules or official guidance to limit how the technology could be used in electoral contexts. Prohibiting problematic uses of generative AI, such as impersonation, can compel political campaigns and candidates to adopt more responsible behavior. Rules that require labeling provide voters with the transparency they need to distinguish between genuine and fabricated content.

Ahead of South Korea's elections, legislators banned the use of deepfakes in campaign materials starting 90 days before the balloting, with offenders subject to penalties of up to seven years in prison or fines of 50 million won ($39,000). The law also required the labeling of AI-generated materials that were published before the 90-day period, and empowered election regulators to order takedowns of offending content. Taiwanese policymakers took a more proportionate approach, passing a June 2023 law that allows candidates to report misleading deepfakes of themselves to social media companies for removal, if technical experts at law enforcement agencies confirm that the content was generated by AI.

In the United States, while no federal rules were adopted, at least 19 state legislatures passed laws to address generative AI in electoral contexts as of July 2024, according to the Brennan

A healthy 21st-century democracy cannot function without a trustworthy online environment, in which free expression and access to diverse information prevail.

Center for Justice. A Michigan law enacted in November 2023 requires labeling of political advertisements generated by AI and introduces criminal penalties for using the technology, without appropriate labels, to "deceive" voters in the 90 days ahead of an election. A Florida law passed in March 2024 amends the state's campaign finance framework to require the labeling of AI-generated content in political ads.

Electoral campaigns in a number of countries deployed generative AI during the coverage period, underscoring the need for clear rules as this technology becomes enmeshed in the ordinary practice of modern politics. Successful Indonesian presidential candidate Prabowo Subianto used an AI-generated avatar to rebrand himself as a cuddly and cat-obsessed figure, appealing to younger voters and effectively papering over credible allegations that he had committed human rights abuses as a military commander before the country's transition to democracy. During Argentina's November 2023 presidential runoff, candidates Javier Milei and Sergio Massa integrated AI-generated memes into their campaigning, most notably when the Massa camp posted an AI-manipulated video that depicted Milei speaking about a private market for the sale of organs, effectively mocking a previous statement he had made.

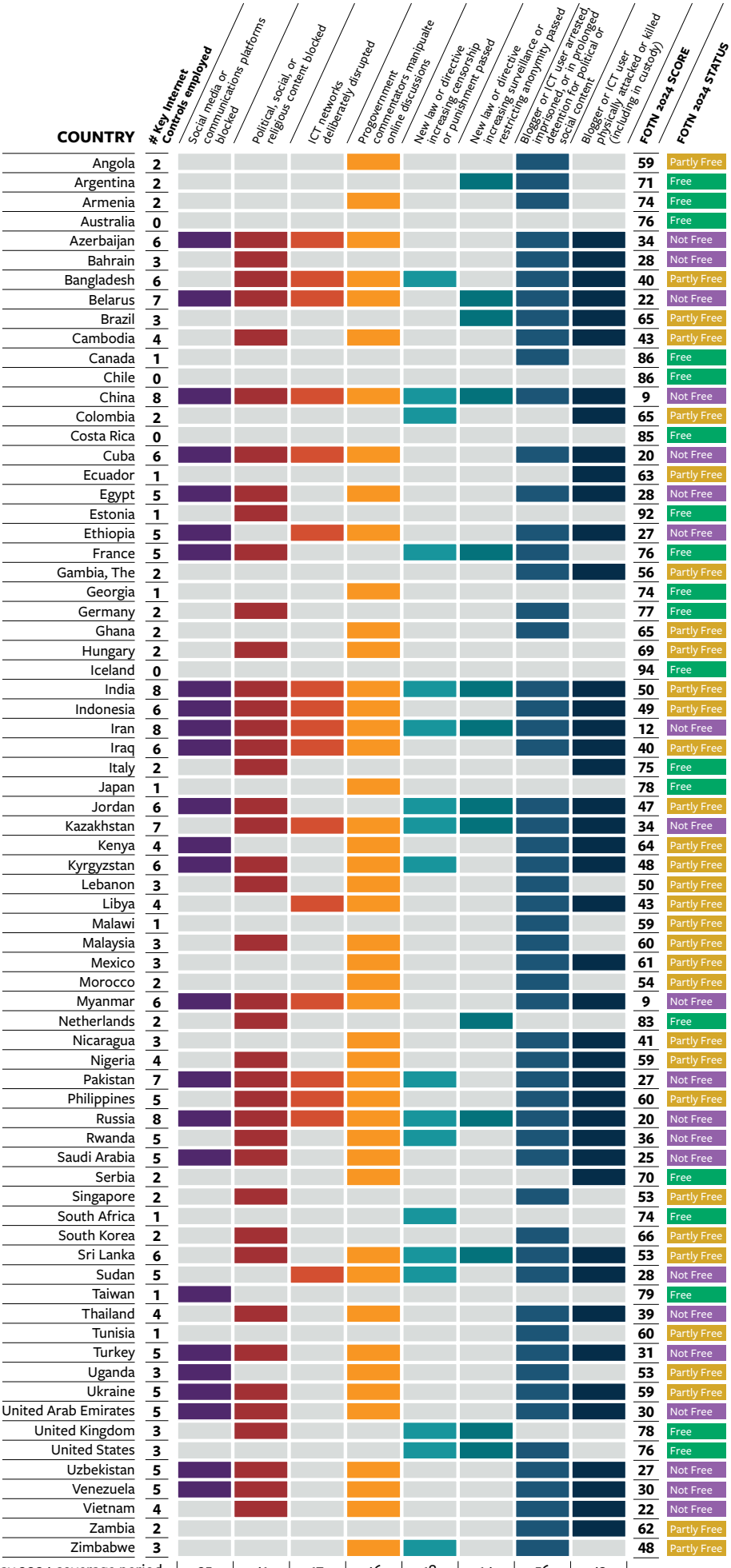
Internet freedom as a pillar of modern democracy

It is no coincidence that the most effective and frequently recommended means for reversing the global decline in internet freedom are also potent safeguards for restoring confidence in the electoral information space. For example, internet regulations that mandate transparency around content moderation systems and provide platform data to vetted researchers can help equip voters with a more informed understanding of influence operations during balloting. Long-term support for civil society groups can empower them with the necessary resources to collaborate with election commissions to boost authoritative voting information and protect free expression. The best solutions also go beyond technology, calling for reinvestment in civic education, modernization of election rules, and accountability for powerful figures who engage in antidemocratic behavior.

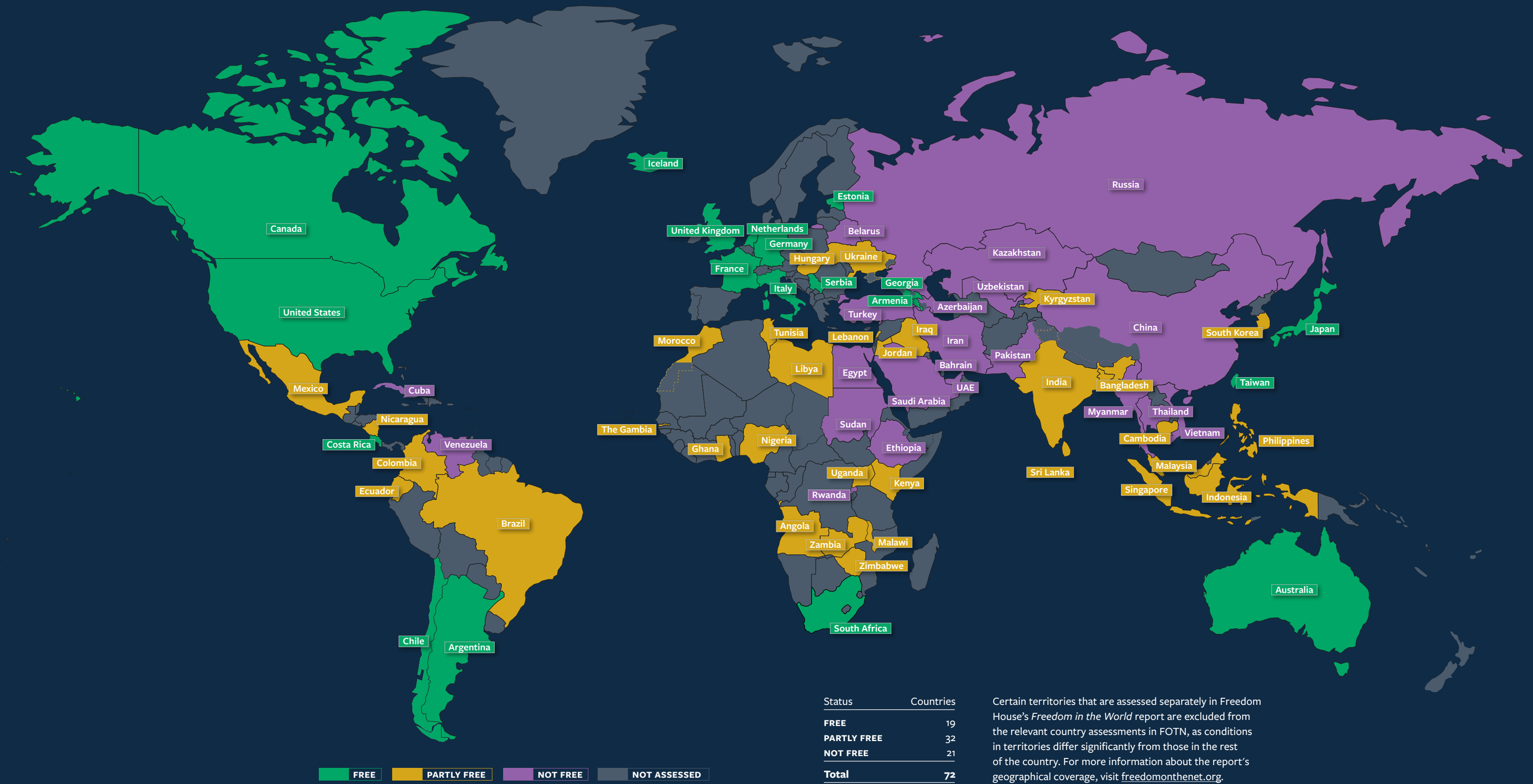
Ultimately, a healthy 21st-century democracy cannot function without a trustworthy online environment, in which freedom of expression and access to diverse information prevail. Defending these foundational rights allows people to safely and freely use the internet to engage in discussion, form civic movements, scrutinize government and company performance, and debate and build consensus around key social challenges. The protection of democracy writ large therefore requires a renewed and sustained commitment to upholding internet freedom around the world.

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 2023 to May 2024. The Key Internet Controls reflect restrictions that do not adhere to international human rights standards.



FREEDOM ON THE NET 2024

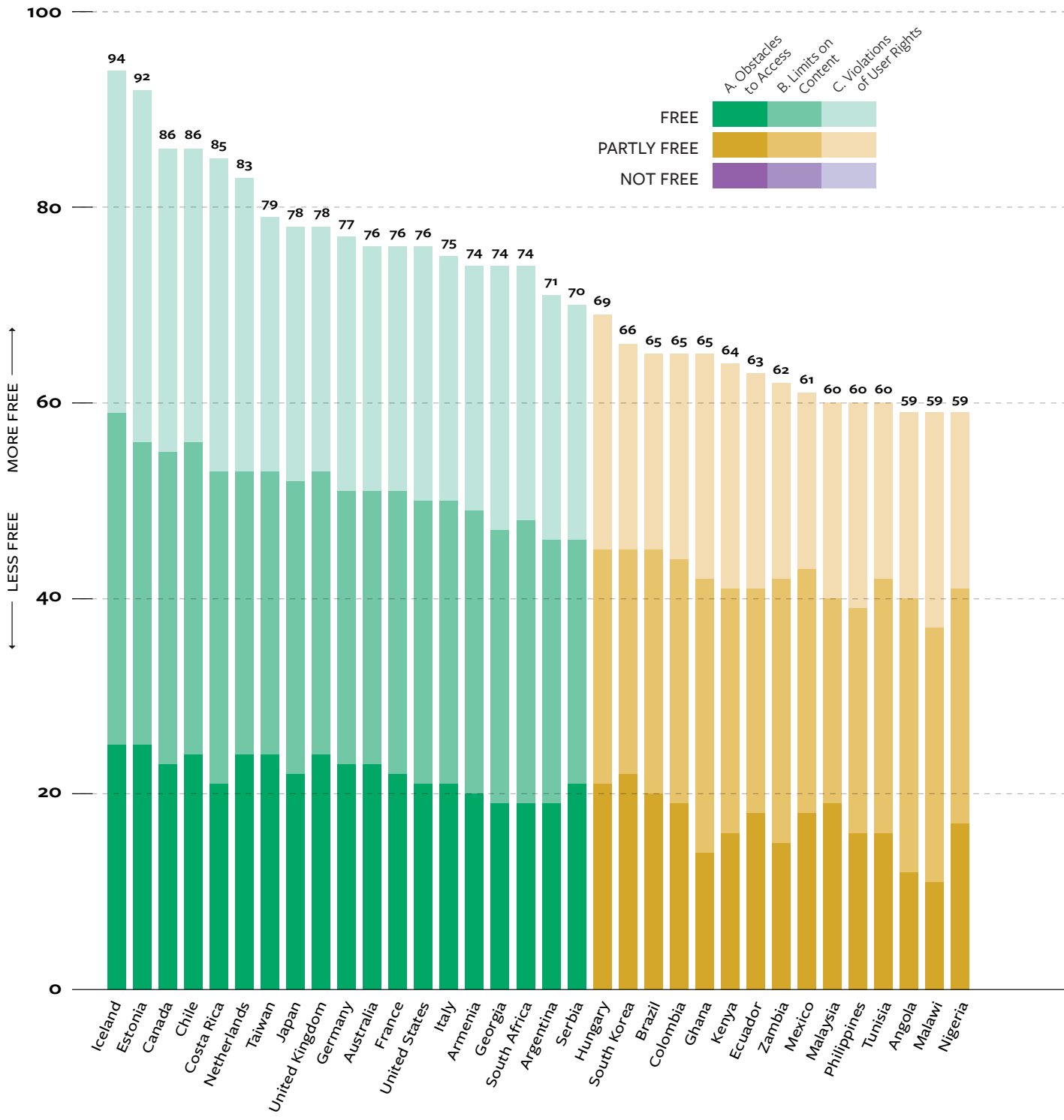


Status	Countries
FREE	19
PARTLY FREE	32
NOT FREE	21
Total	**72**

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



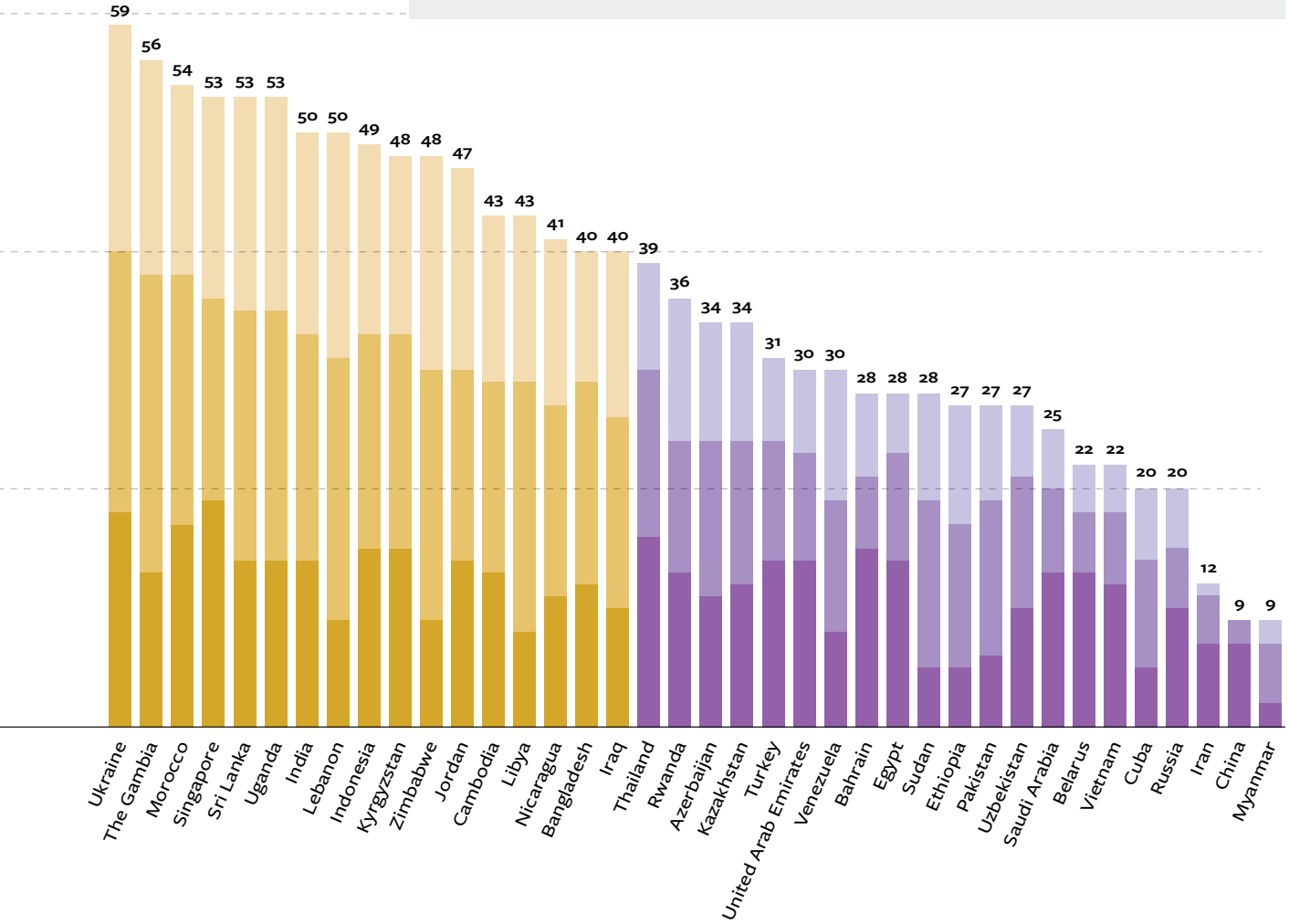
Freedom on the Net 2024 covers 72 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems. Each country receives a numerical score from **100 (the most free)** to **0 (the least free)**, which serves 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.



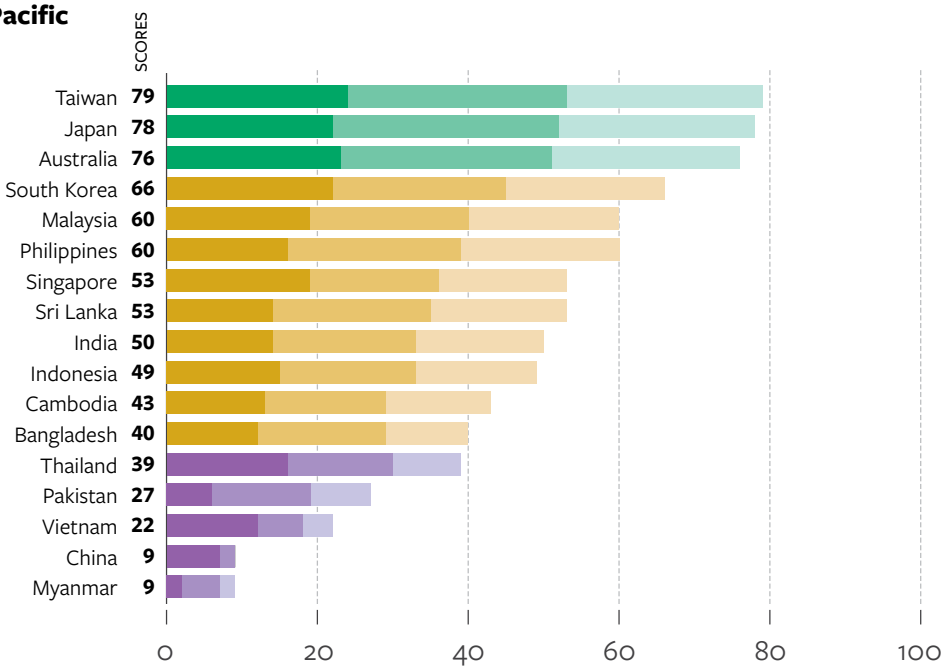
REGIONAL RANKINGS

Freedom on the Net 2024 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.

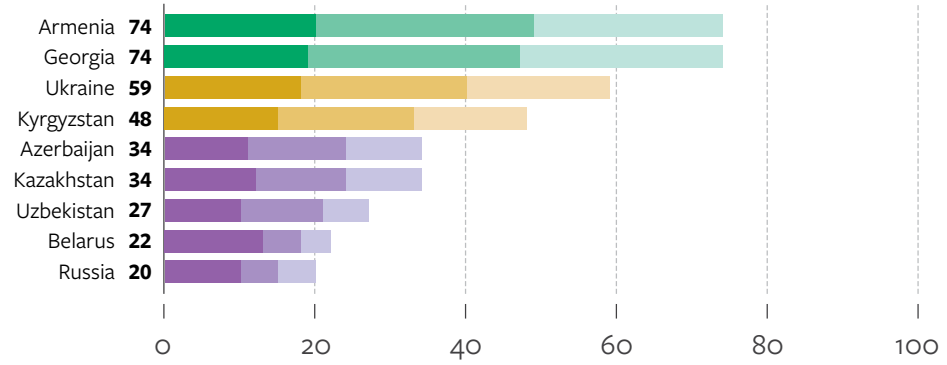
A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights

0 = Least Free
100 = Most Free

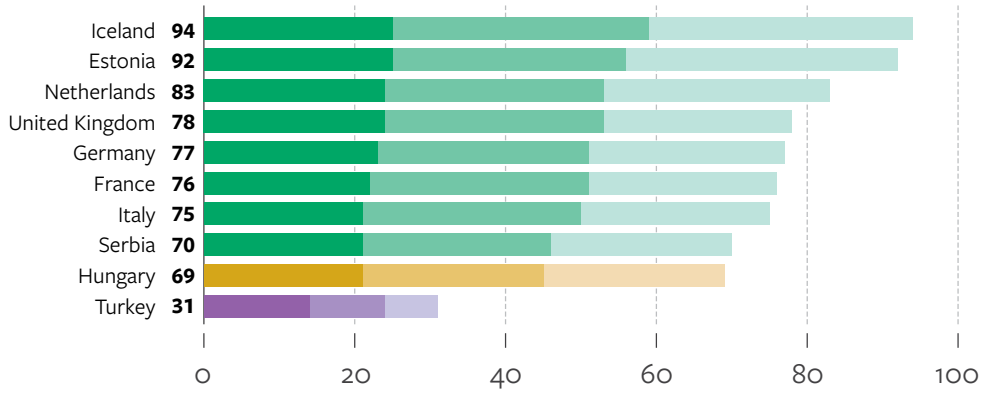
Asia-Pacific



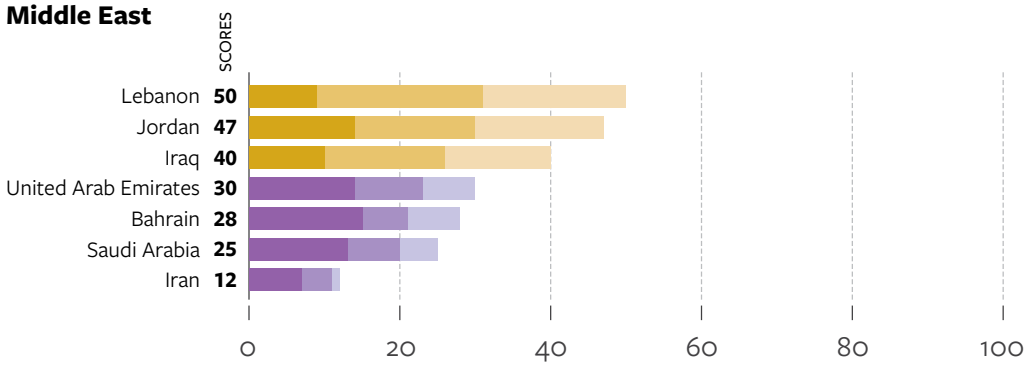
Eurasia



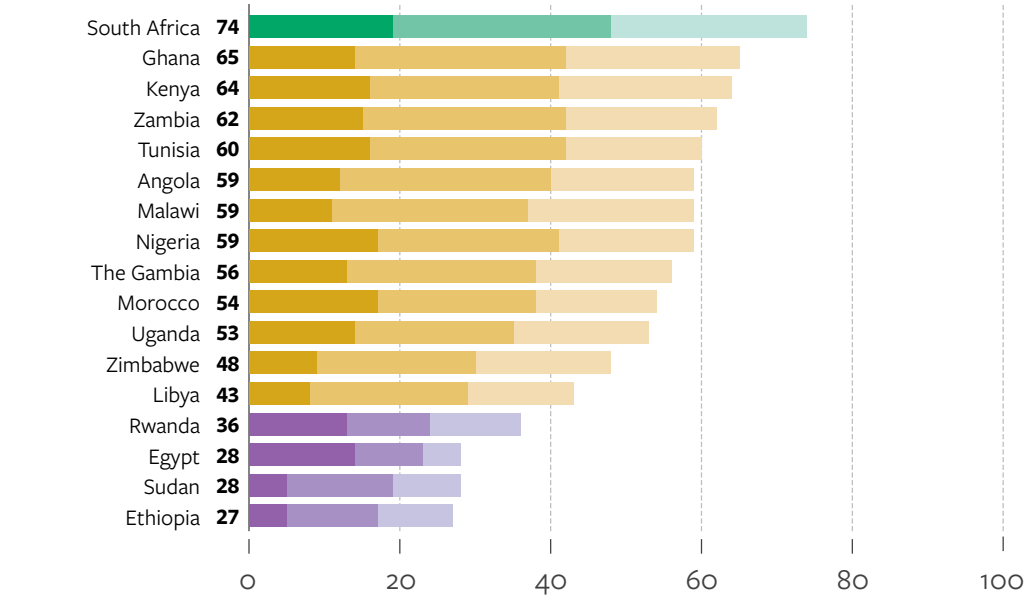
Europe



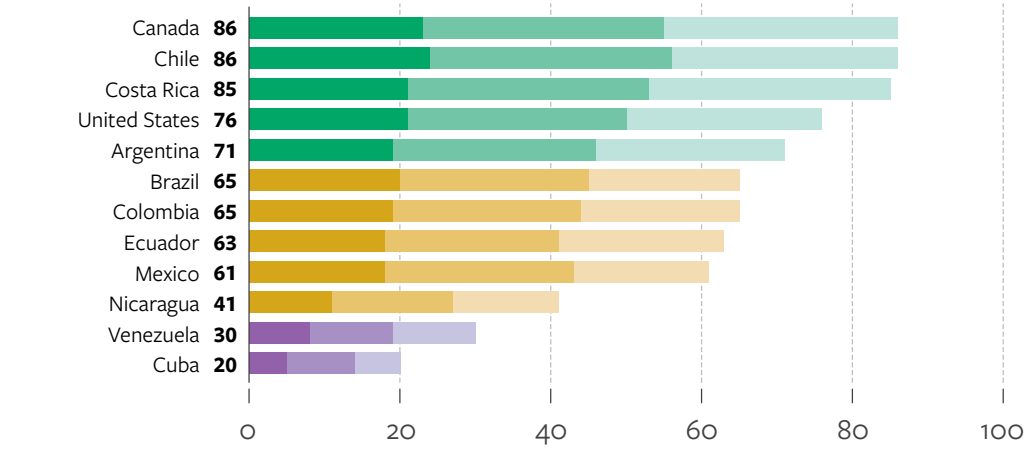
Middle East



Africa



Americas



Policy Recommendations

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

The following recommendations lay out strategies that policymakers, regulators, donor institutions, and private companies can adopt to advance human rights online and prevent or mitigate the internet's contribution to broader societal harms. While reversing the global decline in internet freedom will require the participation of a range of stakeholders, governments and companies should actively partner with civil society, which has always been at the forefront in raising awareness of key problems and identifying remedies with which to address them.

1. PROMOTE FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION

Freedom of expression online is increasingly under attack as governments shut off internet connectivity, block social media platforms, or 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 and access to information.

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 and access to information. 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. Provisions in the European Union's Digital Services Act—notably its transparency requirements, data accessibility for researchers, a coregulatory form of enforcement, and algorithmic accountability—offer a promising model for content-related laws.

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. The Global Network Initiative's Principles provide concrete recommendations on how to do so.

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. DEFEND INFORMATION INTEGRITY

The potential consequences of false, misleading, and incendiary content are especially grave during election periods, underscoring the need to protect information integrity. Efforts to address the problem should start well before campaigning begins and continue long after the last vote is cast.

Governments

Governments should adopt 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 highlights the need to protect freedom of expression and address false or misleading information that targets and affects women, LGBT+ people, people with disabilities, and Indigenous people. It also underscores the importance of working with other initiatives designed to enhance information integrity, such as the Forum on Information and Democracy.

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 information integrity. 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. In addition, election management bodies and/or government officials should seek out trusted community messengers from specific populations who can share reliable information. 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.

Governments should set strong rules on how generative artificial intelligence (AI) can be used in political campaigns. Policymakers should require the labeling of campaign advertisements featuring AI-generated images, audio, or video. Policymakers should also evaluate how to prohibit the use of AI-generated media for manipulative or deceptive purposes in

online campaigning, for example to fabricate statements by a political opponent. In the United States, Congress should direct the Federal Election Commission to pursue rulemaking to this effect, in line with the Federal Communications Commission's pending rulemaking on AI use in campaign advertisements that appear in broadcast media.

Companies

The private sector has a responsibility to ensure that its products contribute to, and do not undermine, a diverse and reliable information space. Companies should invest in staff tasked with work related to public policy, information integrity, 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. 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, disinformation campaigns, and other trends online.

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, such as technical regulators and election management bodies, 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 and procedures 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 to determine whether they are sufficiently protecting human rights.

To combat political violence and support free and fair elections more broadly, technology platforms should develop standards for threat assessment and crisis planning. This includes addressing threats against election workers and responding to false election-related claims by promoting accurate information and meaningfully engaging with civil society, fact-checkers, and, as appropriate, election management bodies and government officials. Companies should dedicate adequate resources to both preelection and postelection activities, and ensure the smooth operation of escalation channels.

3. COMBAT DISPROPORTIONATE GOVERNMENT SURVEILLANCE

Governments worldwide have passed disproportionate surveillance laws and can access a booming commercial market for surveillance tools, giving them the capacity to monitor the private communications of individuals inside and beyond their borders in violation of international human rights standards. The lack of data privacy safeguards in the United States and around the world exacerbates the harms of excessive government surveillance.

Governments

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. 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.

In the United States, lawmakers should reform or repeal existing surveillance laws and practices, including Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, to better align them with these standards. Broad powers under Section 702 and Executive Order 12333 have allowed US government agencies to collect and access Americans' personal data without meaningful transparency or oversight. Congress should also close a legal loophole that allows US government agencies to purchase personal data from commercial brokers rather than obtaining a warrant.

Policymakers should refrain from mandating the introduction of "back doors" to digital devices and services, requiring that messages be traceable, or reducing intermediary liability protections for providers of end-to-end encryption. Weakening encryption would endanger the lives of activists, journalists, members of marginalized communities, and ordinary people around the world.

Governments should restrict the export of surveillance technologies of concern, including commercial spyware, and should solicit input from civil society when considering how to strengthen export controls to protect human rights. The US Commerce Department's Bureau of Industry and Security has taken several important steps to this effect, including adding commercial spyware firms to its Entity List—which subjects them to specific export restrictions—and initiating regular civil society consultations. The US Congress should pass legislation to codify provisions of Executive Order 14093 that prohibit the operational use of commercial spyware products by federal agencies.

The US government should continue to lead the international community in its efforts to combat the abuse of commercial spyware by encouraging signatories to the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware to follow through on their commitments. Like-minded democracies, in Europe and elsewhere, should follow suit, including through the Pall Mall Process led by the United Kingdom and France, among other forums. Bold action from these democracies would be an important step in combating spyware purveyors' irresponsible global trade.

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. Companies should also resist government data requests that contravene international human rights standards or lack a valid judicial warrant. Digital platforms should use all available legal channels to challenge such 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.

Businesses exporting surveillance and censorship technologies that could be used to commit human rights abuses should report publicly and annually on the human rights–related due diligence they are conducting before making sales, the due diligence obligations they are requiring from their resellers and distributors, and their efforts to identify requests from customers that suggest the technologies may be used for repressive purposes. The reports should include a list of countries to which they have sold such technologies. These businesses should also adhere to obligations and responsibilities outlined in the UN Guiding Principles on Business and Human Rights.

4. SAFEGUARD PERSONAL DATA

Comprehensive data-protection regulations and industry policies on data protection are essential for upholding privacy and other human rights online, 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 in which 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.

The US Congress should urgently pass a comprehensive federal law on data privacy that includes data minimization, the principle that personal information should only be collected and stored to the extent necessary for a specific purpose, and purpose limitation, the principle that personal data gathered for one purpose should not later be used for another. This is especially relevant for discussions around generative AI and other technologies that depend on harvesting information online without people's consent.

In the absence of congressional action, the US Federal Trade Commission (FTC) has been working to develop new regulations on commercial surveillance and data security. While an Advance Notice of Proposed Rulemaking was announced over two years ago, the process is still ongoing. The commission should continue to pursue enforcement of existing rules to hold companies accountable, and Congress should ensure that the FTC has sufficient resources to finalize and enforce meaningful new regulations related to data protection.

Companies

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, including what information may be collected from user prompts to generative AI services. Finally, companies should ensure that people who use their services have control over their own information, including the right to access it, delete it, and prevent it from affecting an algorithm's behavior.

5. PROTECT A FREE AND OPEN INTERNET

A successful defense of the free, open, and interoperable internet will depend on international cooperation and a shared vision for global internet freedom. If democracies live up to their own values at home, they will serve as more credible advocates for internet freedom abroad.

Governments

Governments should ensure that digital diplomacy is coordinated among fellow democracies and promotes the protection of internationally recognized human rights. They should identify and utilize regional multilateral forums that are strategically placed

to advance the principles of a free and open internet. Democracies should also facilitate dialogue among national policymakers and regulators, allowing them to share best practices and strengthen joint engagement at international standards-setting bodies.

The multistakeholder model of internet governance, which is essential for the functioning of the global internet and helps constrain the influence of authoritarian regimes on internet freedom, should be protected at multilateral forums and initiatives, including through the United Nations' Global Digital Compact. Governments should renew the mandate of the Internet Governance Forum and its regional iterations during the forthcoming World Summit on Information Society+20 Review in 2025 and help ensure that civil society can meaningfully participate in these discussions.

The Freedom Online Coalition (FOC) should improve its name recognition and its ability to drive diplomatic coordination and global action. The body should more proactively articulate the benefits of a free and open internet to other governments and be more publicly and privately vocal about threats and opportunities for human rights online. The FOC should also create an internal mechanism by which member states' laws, policies, and activities can be evaluated to ensure that they align with the coalition's principles. Finally, the FOC should continue to diversify and expand its advisory network.

Governments should establish internet freedom programming as a vital component of their democracy assistance strategies, incorporating funding for cybersecurity and digital hygiene into their projects. Program beneficiaries should receive support for open-source and user-friendly technologies that will help them circumvent government censorship, protect themselves against surveillance, and overcome restrictions on connectivity. When new and emerging technologies, such as generative AI, are harnessed for programming, they should be deployed in a rights-respecting way.

Democracies should coordinate to ensure that perpetrators who direct or engage in reprisals against people for their online speech face meaningful accountability. This could include imposing targeted sanctions or blocking or revoking visas. Sanctions against state entities should be crafted to minimize their impact on ordinary citizens, and when broad-based sanctions are imposed, democratic governments should carve out exemptions for internet services when relevant.

Governments should advocate for the immediate, unconditional release of those imprisoned or detained for online expression that is protected under international human rights standards. Governments should incorporate these cases, in addition to broader internet freedom concerns, into bilateral and multilateral engagement with perpetrator states.

Companies

Companies should engage in continuous dialogue with civil society to understand the effects of their policies and products. They should seek out local expertise on the political and cultural context in markets where they have a presence or where their products are widely used, especially in repressive settings that present unique human rights challenges. Consultations with civil society groups should inform companies' decisions to operate in a particular country, their approach to local content moderation, and their development of policies and practices—particularly during elections or crisis events, when managing government requests, and when working to counter online harms.

Prior to launching new internet-related or AI services or expanding them to a new market, companies should conduct and publish human rights impact assessments to fully illuminate the ways in which their products and actions might affect rights including freedom of expression, freedom from discrimination, and privacy.

Finally, when complying with sanctions and anti–money laundering regulations, companies should coordinate with democratic governments to ensure that their risk mitigation efforts are not negatively and needlessly affecting civilians who have not themselves been sanctioned.

What We Measure

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

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

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

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

THE RESEARCH AND SCORING PROCESS

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

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

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

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

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

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

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

Checklist of Questions

A. OBSTACLES TO ACCESS

(*0–25 POINTS*)

1. **Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?** (*0–6 points*)
   - Do individuals have access to high-speed internet services at their home, place of work, 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, such as zero-rating plans, 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 service 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?
   - Are oversight bodies, such as those governed by the state or industry-created mechanisms, effective at ensuring content protected under international human rights standards is not removed?

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?
   - Does disinformation, coordinated by foreign or domestic actors for political purposes, have a significant impact on public debate?

6. **Are there economic, regulatory, or other constraints that negatively affect 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 misinformation undermine users' ability to access independent, credible, and diverse sources of information?
   - Does false or misleading content online significantly contribute to offline harms, such as harassment, property destruction, physical violence, or death?
   - If there is extensive censorship, do users employ 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, including 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, including 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, 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 to protect their communications?
   - 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 local authorities such as police departments surveil people's communications (including through International Mobile Subscriber Identity-Catchers or IMSI catcher technology), and if so, are such practices subject to rigorous guidelines and judicial oversight?
   - Do state actors use artificial intelligence and other advanced technology for the purposes of online surveillance, without appropriate oversight?

- Do 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, 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 staff and a network of more than 95 independent researchers, who come from civil society organizations, academia, journalism, and other backgrounds, covering 72 countries. In repressive environments, Freedom House takes care to ensure researchers' anonymity and/or works with experts living abroad.

Freedom House 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, The Dutch Postcode Lottery, Google, Internet Society, The New York Community Trust, the U.S. State Department's Bureau of Democracy, Human Rights, and Labor (DRL), and Verizon.

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

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
- **Kian Vesteinsson**, Senior Research Analyst for Technology and Democracy
- **Grant Baker**, Research Analyst for Technology and Democracy
- **Aashna Agarwal**, Research Associate for Technology and Democracy
- **Matthew Barak**, Research Associate
- **Mina Loldj**, Research Associate, Free Them All: The Fred Hiatt Program to Free Political Prisoners
- **Maddie Masinsin**, Community Engagement Specialist for Technology and Democracy
- **Elizabeth Sutterlin**, Research Associate for Technology and Democracy

Amelia Larson, David Meijer, Shannon O'Toole, Tyler Roylance, and Lora Uhlig edited *Freedom on the Net*. Gerardo Berthin, Nicole Bibbins Sedaca, Annie Boyajian, Yana Gorokhovskaia, Nate Schenkkan, Adrian Shahbaz, Lara Shane, and Yaqiu Wang provided valuable feedback on the summary of findings. Clara Apt, Phumelele Mncina, César Augusto Portocarrero Rodríguez, Rachel Simroth, Nodari Tsaava, and Jessica White provided research assistance.

Report authors

- **Argentina:** Eduardo Ferreyra, independent researcher
- **Armenia:** Samvel Martirosyan, Co-Founder of CyberHUB
- **Australia:** Lizzie O'Shea and Samantha Floreani, Digital Rights Watch
- **Azerbaijan:** Arzu Geybulla, independent researcher
- **Bangladesh:** Rezwan I., independent researcher
- **Brazil:** Artur Pericles Lima Monteiro, Schmidt Visiting Scholar, Yale Jackson School of Global Affairs; Resident Fellow, Information Society Project, Yale Law School; Affiliated Researcher, Constitution, Law & Politics Group, University of São Paulo
- **Canada:** Allen Mendelsohn, McGill University
- **Chile:** Danielle Zaror M., law professor at Universidad de Chile
- **Colombia:** Susana Echavarría Medina and Emmanuel Vargas Penagos, El Veinte
- **Costa Rica:** Óscar Mario Jiménez Alvarado, Fernando José Martínez de Lemos, Johanna Rodríguez López, Programa de Libertad de Expresión y Derecho a la Información (PROLEDI)
- **Cuba:** Ted A. Henken, Baruch College, City University of New York
- **Ecuador:** Emily Fonseca-Jácome and Margarita Yépez-Villareal, Fundación Datalat
- **Estonia:** Hille Hinsberg and Florian Marcus, Proud Engineers
- **Ethiopia:** Atnafu Brhane, independent researcher
- **France:** Audrey Cerrone, independent researcher
- **Georgia:** Teona Turashvili, Institute for Development of Freedom of Information (IDFI)
- **Germany:** Matthieu Binder and Raphael Hadadi, iRights.Lab
- **Hungary:** Dalma Dojcsák, Hungarian Civil Liberties Union
- **Iceland:** Arnaldur Sigurðarson, independent researcher

- **Indonesia:** Southeast Asia Freedom of Expression Network (SAFEnet)
- **Iraq:** Asia Abdulkareem Anwer and Hayder Hamzoz, INSM
- **Italy:** Philip Di Salvo and Antonella Napolitano, independent researchers
- **Japan:** Hamada Tadahisa, Japan Computer Access for Empowerment
- **Kazakhstan:** Adil Nurmakov, independent researcher
- **Malawi:** Jimmy Kainja, University of Malawi
- **Malaysia:** Siti Nurliza Samsudin and Kelly Koh, Sinar Project
- **Mexico:** Vladimir Cortés Roshdestvensky, independent researcher
- **Myanmar:** Oliver Spencer, independent researcher
- **Nicaragua:** IPANDETEC and Jenny Galindo, independent researcher
- **Nigeria:** Adeboro Odunlami, independent researcher
- **Philippines:** Vino Lucero, independent researcher
- **Serbia:** Mila Bajić and Bojan Perkov, SHARE Foundation
- **Singapore:** Kirsten Han, independent researcher
- **South Africa:** Tshepiso Hadebe, independent researcher
- **South Korea:** Yenn Lee, SOAS University of London
- **Sudan:** Digital Rights Lab
- **Thailand:** Emilie Palamy Pradichit and Ploypitcha Uerfuer, Manushya Foundation
- **The Gambia:** Nasiru Deen, independent researcher
- **The Netherlands:** Bits of Freedom
- **Turkey:** Gürkan Özturan, European Centre for Press and Media Freedom
- **Uganda:** Lillian Nalwoga, independent researcher
- **Ukraine:** Olga Kyryliuk, independent researcher
- **United Kingdom:** Dr. Edina Harbinja, Aston University
- **United States:** Rachel Lau, independent researcher
- **Uzbekistan:** Ernest Zhanaev, independent researcher
- **Vietnam:** Trinh Hữu Long, Legal Initiatives for Vietnam
- **Zambia:** Bulanda T. Nkhowani, independent researcher

Researchers for Angola, Bahrain, Belarus, Cambodia, China, Egypt, Ghana, India, Iran, Jordan, Kenya, Kyrgyzstan, Lebanon, Libya, Morocco, Pakistan, Russia, Rwanda, Saudi Arabia, Sri Lanka, Taiwan, Tunisia, the United Arab Emirates, Venezuela, and Zimbabwe wished to remain anonymous.

Advisers

- **Sarah Bauerle Danzman**, independent researcher
- **Mert Bayar**, Postdoctoral Scholar, Center for an Informed Public at the University of Washington
- **Eto Buziashvili**, Digital Forensic Research Lab, Atlantic Council
- **Hakeem Dawd Qaradaghi**, independent researcher
- **Alena Epifanova**, Research Fellow at Center for Order and Governance in Eastern Europe, Russia, and Central Asia, German Council on Foreign Relations
- **Marwa Fatafta**, Middle East and North Africa Policy and Advocacy Director, Access Now
- **Smitha Krishna Prasad**, Fritz Fellow, Georgetown University Law Center
- **J. Carlos Lara**, independent researcher
- **Miaan Group**
- **Matt Perault**, Director, Center on Technology Policy, UNC-Chapel Hill
- **Beatriz Saab**, independent researcher
- **Stephanie Sugars**, Senior Reporter, U.S. Press Freedom Tracker
- **Danielle Tomson**, Researcher Manager, Center for an Informed Public at the University of Washington
- **Qiang Xiao**, Founder and Editor-in-Chief of China Digital Times and research scientist at the School of Information, University of California Berkeley

A NOTE ON ADDITIONAL SOURCES AND DATA

This report's main essay, data points, and policy recommendations were informed by the individual *Freedom on the Net* country reports, written by the external report authors and reviewed by the external advisers who are listed above. In addition, Freedom House staff conducted desk research, held one-on-one interviews and group roundtables, and drew on the important work of various media groups, civil society organizations, and other experts. Freedom House extends appreciation to Jamil Assis, William Bird, Cloudflare, Eve Chiu, Renee DiResta, Dean Jackson, Billion Lee, Zoe Lee, the Open Observatory of Network Interference, Chris Roper, Yoel Roth, Vakau, Chihhao Yu, and others who prefer to remain anonymous. Freedom House also thanks the multistakeholder group of experts who attended a roundtable on internet freedom trends, including Matt Bailey, Jon Bateman, Patrick Day, Kat Duffy, Alyson K. Finley, Jared Ford, Josh A. Goldstein, Katie Harbath, Matt Perault, Jason Pielemeier, Lisa Poggiali, Alexandria Walden, Alex Warofka, and Moira Whelan.

Country-specific data and sources used in the report's essay can be downloaded at freedomonthenet.org, and each country report and its relevant footnotes are available at https://freedomhouse.org/countries/freedom-net/scores.

HOW TO CITE THIS REPORT

Funk, Vesteinsson, Baker, Brody, Grothe, Agarwal, Barak, Loldj, Masinsin, Sutterlin eds. *Freedom on the Net 2024*, Freedom House, 2024, freedomonthenet.org.

Funk, Vesteinsson, and Baker, "The Struggle for Trust Online," in Funk, Vesteinsson, Baker, Brody, Grothe, Agarwal, Barak, Loldj, Masinsin, Sutterlin eds. *Freedom on the Net 2024*, Freedom House, 2024, freedomonthenet.org.

"Angola," in Funk, Vesteinsson, Baker, Brody, Grothe, Agarwal, Barak, Loldj, Masinsin, Sutterlin eds. *Freedom on the Net 2024*, Freedom House, 2024, freedomonthenet.org.

Board of Trustees

* Denotes members of the Executive Board

Interim President
Nicole Bibbins Sedaca

Co-Chairs
The Hon. Jane Harman
Wendell L. Willkie, II

Vice Chair
Goli Ameri*
Peter Bass*

Treasurer
Robert Keane*

Secretary
Cater Lee*

Trustees
Carol C. Adelman*
Sewell Chan
Michael Chertoff*
Carole Corcoran
Deborah Cowan
Rodger Desai
Martin Etchevers
Mathea Falco
David L. Fogel
Francis Fukuyama
Jonathan Ginns
Mark Goodman*
Dionisio Gutierrez
Nina Jacobson
Thomas Kahn*
Conrad Kiechel
Rachel Kleinfeld*
Howard Konar
Felix Maradiaga
Dr. Sharon S. Nazarian
Sushma Palmer
Maurice A. Perkins
Bill Reichblum
Collin Roche
Ian Simmons*
Thomas Staudt*
Reed V. Tuckson
Robert H. Tuttle
Joseph Votel
Norman Willox*

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

Freedom House

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
@freedomonthenet
202.296.5101
info@freedomhouse.org