Freedom House

FREEDOM ON THE NET 2023

The Repressive Power of Artificial Intelligence

FREEDOM ON THE NET 2023

TABLE OF CONTENTS

Key Findings 1

Freedom on the Net 2023: The Repressive Power of Artificial Intelligence 2

Generative AI Supercharges Disinformation 8

Governments Harness AI to Reinforce Censorship 13

Regulating AI to Protect Internet Freedom 19

Recommendations 30

Methodology 36

Checklist of Questions 37

Acknowledgements and Sources 43

TABLES, CHARTS, AND GRAPHICS

Global Internet Population by 2023 FOTN Status 2

Automating Digital Repression: How AI Can Harm Human Rights 3

An Arsenal of Tactics for Digital Election Interference 5

Global Internet User Stats 6

Glossary of AI Terms 8

Harnessing AI to Augment Disinformation Campaigns 10

Tried and True: Conventional Censorship Methods Proliferate 16

Ensuring AI Advances Internet Freedom 21

Key Internet Controls by Country 23

Freedom on the Net 2023 Map 24

Global Rankings 26

Regional Rankings 28

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

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

This booklet is a summary of findings for the 2023 edition of *Freedom on the Net*. Narrative reports on the 70 countries assessed in this study can be found on our website at freedomonthenet.org.

ON THE COVER

Illustration by Mitch Blunt

Key Findings

1

Global internet freedom declined for the 13th consecutive year. Digital repression intensified in Iran, home to this year's worst decline, as authorities shut down internet service, blocked WhatsApp and Instagram, and increased surveillance in a bid to quell antigovernment protests. Myanmar came close to dislodging China as the world's worst environment for internet freedom, a title the latter country retained for the ninth consecutive year. Conditions worsened in the Philippines as outgoing president Rodrigo Duterte used an antiterrorism law to block news sites that had been critical of his administration. Costa Rica's status as a champion of internet freedom has been imperiled after the election of a president whose campaign manager hired online trolls to harass several of the country's largest media outlets.

2

Attacks on free expression grew more common around the world. In a record 55 of the 70 countries covered by *Freedom on the Net*, people faced legal repercussions for expressing themselves online, while people were physically assaulted or killed for their online commentary in 41 countries. The most egregious cases occurred in Myanmar and Iran, whose authoritarian regimes carried out death sentences against people convicted of online expression-related crimes. In Belarus and Nicaragua, where protections for internet freedom plummeted during the coverage period, people received draconian prison terms for online speech, a core tactic employed by longtime dictators Alyaksandr Lukashenka and Daniel Ortega in their violent campaigns to stay in power.

3

Generative artificial intelligence (AI) threatens to supercharge online disinformation campaigns. At least 47 governments deployed commentators to manipulate online discussions in their favor during the coverage period, double the number from a decade ago. Meanwhile, AI-based tools that can generate text, audio, and imagery have quickly grown more sophisticated, accessible, and easy to use, spurring a concerning escalation of these disinformation tactics. Over the past year, the new technology was utilized in at least 16 countries to sow doubt, smear opponents, or influence public debate.

4

AI has allowed governments to enhance and refine their online censorship. The world's most technically advanced authoritarian governments have responded to innovations in AI chatbot technology, attempting to ensure that the applications comply with or strengthen their censorship systems. Legal frameworks in at least 22 countries mandate or incentivize digital platforms to deploy machine learning to remove disfavored political, social, and religious speech. AI, however, has not completely displaced older methods of information control. A record 41 governments blocked websites with content that should be protected under free expression standards within international human rights law. Even in more democratic settings, including the United States and Europe, governments considered or actually imposed restrictions on access to prominent websites and social media platforms, an unproductive approach to concerns about foreign interference, disinformation, and online safety.

5

To protect internet freedom, democracy's supporters must adapt the lessons learned from past internet governance challenges and apply them to AI. AI can serve as an amplifier of digital repression, making censorship, surveillance, and the creation and spread of disinformation easier, faster, cheaper, and more effective. An overreliance on self-regulation by private companies has left people's rights exposed to a variety of threats in the digital age, and a shrinking of resources in the tech sector could exacerbate the deficiency. To protect the free and open internet, democratic policymakers—working side by side with civil society experts from around the world—should establish strong human rights–based standards for both state and nonstate actors that develop or deploy AI tools.

Freedom on the Net 2023: The Repressive Power of Artificial Intelligence

By Allie Funk, Adrian Shahbaz, and Kian Vesteinsson

Advances in artificial intelligence (AI) are amplifying a crisis for human rights online. While AI technology offers exciting and beneficial uses for science, education, and society at large, its uptake has also increased the scale, speed, and efficiency of digital repression. Automated systems have enabled governments to conduct more precise and subtle forms of online censorship. Purveyors of disinformation are employing AI-generated images, audio, and text, making the truth easier to distort and harder to discern. Sophisticated surveillance systems rapidly trawl social media for signs of dissent, and massive datasets are paired with facial scans to identify and track prodemocracy protesters.

These innovations are reshaping an internet that was already under serious threat. Global internet freedom declined for the 13th consecutive year in 2023. Of the 70 countries covered by *Freedom on the Net*, conditions for human rights online deteriorated in 29, while only 20 countries registered overall gains. For the ninth consecutive year, China was found to have the worst conditions for internet freedom, though Myanmar came close to surpassing it. The year's largest decline occurred in Iran, followed first by the Philippines and then by Belarus, Costa Rica, and Nicaragua. In more than three-fourths of the countries covered by the project, people faced arrest for simply expressing themselves online. And governments in a record 41 countries resorted to censoring political, social, or religious content.

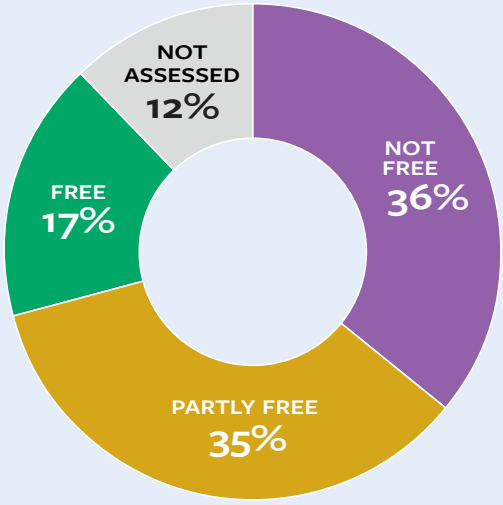
Many observers have debated the existential risks posed by future AI advances, but these should not be allowed to overshadow the ways in which the cutting-edge technology is undermining internet freedom today. Democratic policymakers should establish a positive regulatory vision for the design and deployment of AI tools that is grounded in human rights standards, transparency, and accountability. Civil society experts, the drivers of so much progress for human rights in the digital age, should be given a leading role in policy development and the resources they need to keep watch over these systems. AI carries a significant potential for harm, but it can also be made to play a protective role if the democratic community learns the right lessons from the past decade of internet regulation.

Major declines

As the novelty of AI chatbots captured much of the public's attention, people around the world struggled against a surge of crude digital repression. Nowhere was this clearer than in Iran, which earned the largest score decline of this year's

GLOBAL INTERNET POPULATION BY 2023 FOTN STATUS

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



AUTOMATING DIGITAL REPRESSION: HOW AI CAN HARM HUMAN RIGHTS

Without robust safeguards and oversight, AI can make censorship, surveillance, and the creation and spread of disinformation easier, faster, cheaper, and more effective.

coverage period. After the death in custody of Jina Mahsa Amini sparked nationwide protests in September 2022, the regime intermittently restricted internet connectivity and blocked WhatsApp and Instagram, the only international social media platforms that had been accessible in the country. But state repression was not limited to the protests: two people were executed for alleged blasphemy after they shared their religious views on Telegram.

Harsh crackdowns on free expression were also routine in China, which retained its title as the worst environment for internet freedom for the ninth year in a row. Among the many people imprisoned for sharing their views online, prominent civic activist and blogger Xu Zhiyong was sentenced to 14 years in prison in April 2023. Meanwhile, censors scrubbed away criticism of the declining economy and discussion of the legislature's rubber-stamp approval of an unprecedented third presidential term for Xi Jinping. Despite such intense repression, the Chinese people showed inspiring resilience. In November 2022, for example, protests over a deadly fire in Urumqi, the toll of which was reportedly made worse by overly restrictive COVID-19 lockdown measures, grew into one of the most open challenges to the ruling Chinese Communist Party (CCP) in decades, triggering a rare nationwide policy reversal by the central government. People employed creative language on social media to evade censors, launching hashtags like "A4" and "white paper exercise" to evoke the blank sheets of paper that demonstrators raised to protest the extremity of CCP censorship.

Myanmar was the world's second most repressive environment for internet freedom this year. Under military rule since a 2021 coup, the country's internet users continued to express support for the democratic resistance movement or grief for the victims of the junta's violence, all at great personal risk to themselves. The army and its informants used Telegram groups to share information on such dissidents, allowing the authorities to identify, detain, and in some

> For the ninth consecutive year, China was found to have the worst conditions for internet freedom, though Myanmar came close to surpassing it.

The September 2022 death of Jina Mahsa Amini in police custody sparked protests across Iran. Pictured is a flyer posted in Canada drawing attention to Iranian authorities' repression. (*Katherine Cheng/SOPA Images via ZUMA Press Wire*)

cases forcibly disappear them. In the most egregious case from the coverage period, the military executed prominent activist Kyaw Min Yu, better known as Ko Jimmy, in July 2022, after arresting him for prodemocracy social media posts. Officials also forced the sale of the last internet service provider in Myanmar that had a degree of independence to a state-linked company in September 2022, clearing the way for implementation of the regime's censorship without resistance from the private sector.

In a record 55 countries this year, people faced legal repercussions for expressing themselves online. The number of countries in which authorities carry out widespread arrests and impose multiyear prison terms for online activity has sharply increased over the past decade, from 18 in 2014 to 31 in 2023. Belarus received the year's third-largest score decline, alongside Costa Rica and Nicaragua. A Belarusian court sentenced Maryna Zolatava and Liudmila Chekina—the editor in chief and director general, respectively, of TUT.by, Belarus's largest independent media outlet—to 12 years in prison for their reporting. In several cases in Nicaragua, President Daniel Ortega's government forced people who had been incarcerated in part for their critical speech online to choose between staying in prison and being sent into exile without their citizenship. Roman Catholic bishop Rolando José Álvarez Lagos, who had his citizenship revoked but refused to leave Nicaragua, received a 26-year prison sentence for broadcasting prayers on social media about authorities' crackdown on Catholic clergy, among other offenses.

This is the 13th edition of *Freedom on the Net*, an annual study of human rights online. The project assesses internet freedom in 70 countries, accounting for 88 percent of the world's internet users. This report covers developments between June 2022 and May 2023. More than 85 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 *Freedom on the Net* website features in-depth reports and data on each country's conditions.

Elections as a flashpoint for digital repression

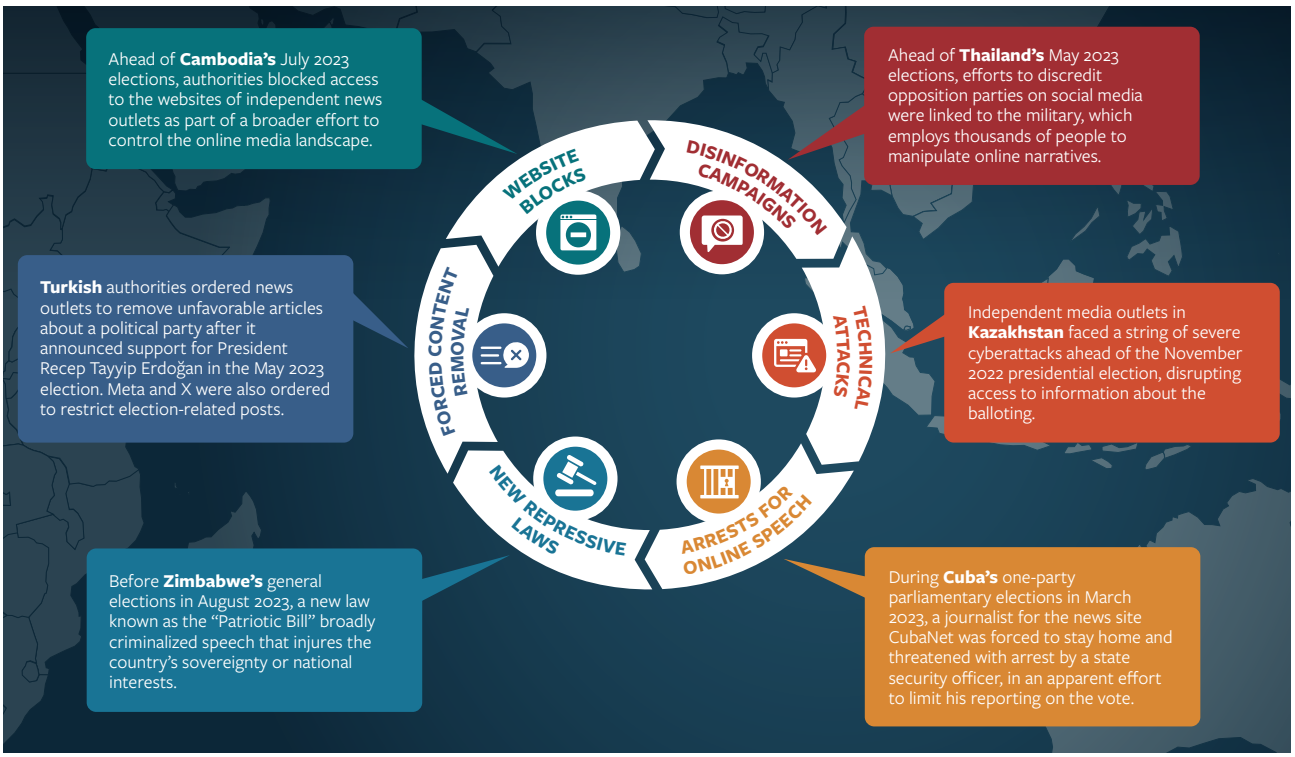
Ahead of and during electoral periods, many incumbent leaders criminalized broad categories of speech, blocked access to independent news sites, and imposed other controls over the flow of information to sway balloting in their favor. In the lead-up to July 2023 elections in Cambodia, through which longtime prime minister Hun Sen engineered a transfer of power to his son, authorities blocked access to the news outlets Radio Free Asia, Voice of Democracy, and *Cambodia Daily*, further cementing the regime's control over the online media landscape. The Turkish government, led for 20 years by Recep Tayyip Erdoğan and his Justice and Development Party (AKP), enacted a repressive law on disinformation and then wielded it against journalists and a member of the opposition ahead of May 2023 general elections. In November 2022, as Tunisian president Kaïs Saïed prepared to hold the first elections under a new constitution that greatly expanded his own power, authorities threatened an independent news site and detained its director over reporting that criticized the government.

Newly elected leaders also sought to reshape the online environment to their benefit. The Philippines suffered this year's second-largest decline in internet freedom. After winning office in last year's election, President Ferdinand "Bongbong" Marcos Jr., son of a Cold War–era dictator, signed a law in October 2022 that required all Filipinos to register their SIM cards under their real name, undermining anonymous communication in what remains a dangerous environment for journalists and activists. Marcos also left in place a blocking order that restricted 27 websites, including several news outlets known for critical reporting; it had first been imposed by outgoing president Rodrigo Duterte in June 2022, under an antiterrorism law that has been a frequent tool of government overreach.

Despite being one of the best performers in *Freedom on the Net*, Costa Rica experienced a recession in internet freedom under the new administration of President Rodrigo

AN ARSENAL OF TACTICS FOR DIGITAL ELECTION INTERFERENCE

Ahead of and during electoral periods, many political leaders increased their control over the information space in a bid to sway balloting in their favor.



GLOBAL INTERNET USER STATS

Almost **4.9 billion** people have access to the internet.

According to Freedom House estimates:

78% live in countries where individuals were arrested or imprisoned for posting content on political, social, or religious issues.

68% live in countries where authorities deployed progovernment commentators to manipulate online discussions.

67% live in countries where individuals have been attacked or killed for their online activities since June 2022.

66% live in countries where websites hosting political, social, or religious content were blocked.

54% live in countries where access to social media platforms was temporarily or permanently restricted.

46% live in countries where authorities disconnected internet or mobile networks, often for political reasons.

Chaves Robles. Self-censorship reportedly increased as his government engaged in harassment of journalists, opposition politicians, and other critics. In one high-profile scandal, the health minister resigned in February 2023 after it was revealed that she had paid someone to harass journalists at three news outlets who reported on government mismanagement.

The coming year will feature a number of consequential elections around the world, and some governments are already attempting to suppress unfavorable speech online. Ahead of Mexico's July 2024 presidential election, term-limited incumbent Andrés Manuel López Obrador has used his office to fuel online harassment campaigns against opposition figures and undermine the independent election authority, presumably to ensure victory for his party's candidate.

Bright spots

Iceland remained the best environment for internet freedom for the fifth consecutive year, followed by Estonia. Sri Lanka earned this year's largest score improvement after authorities did not repeat blocking of social media platforms that had been imposed in April 2022 during mass antigovernment protests. While The Gambia is still ranked Partly Free, it has experienced the most significant improvement over the past decade in *Freedom on the Net*. The country's trajectory demonstrates how broader efforts to rebuild democratic institutions after a period of repression can also benefit internet freedom.

Digital activism and civil society advocacy drove real-world improvements for human rights during the coverage period. Online mobilization helped fuel the Georgian people's movement against a dangerous bill that would have forced civil society groups to register as "foreign agents" if they received more than 20 percent of their funding from abroad. The bill was widely criticized for its similarities to a Russian law. Technology experts in Taiwan notched a victory for transparency after their investigations prompted authorities to admit that police had sidestepped a requirement to seek judicial oversight for website blocks.

The judiciary continued to serve as a bulwark for internet freedom in many countries. In June 2022, Argentina's highest court reinforced the right of access to information when it struck down a celebrity's attempt to remove links to news

articles about her connection to a corruption scandal from Google search results in the country. Three months later, India's Supreme Court ordered the government to explain how it determines when to restrict internet access during school exams to counter cheating; the ruling may bring greater clarity to the country's murky censorship regime. Although Uganda's government introduced repressive restrictions on online speech during the coverage period—including a law that imposes 20-year prison terms for sharing information about same-sex sexual conduct—the Constitutional Court intervened in January 2023 to repeal a section of the Computer Misuse Act that had been used to imprison people for their critical expression online.

Also during the coverage period, concerted policy action against spyware technology was carried forward by an ongoing flood of revelations about the extent to which human rights defenders, journalists, and government officials have been targeted by the tools. The administration of US president Joseph Biden stood out as a global leader in March 2023, when it issued an executive order barring federal agencies from using commercial spyware that poses a threat to national security or counterintelligence, or that could be employed by foreign governments to violate human rights or target Americans. Months later, US officials also added the spyware firms Intellexa and Cytrox to its Entity List, constraining their ability to do business with US companies in certain circumstances. Finally, 11 democracies—including the United States, Costa Rica, and several European countries—agreed to limit the use of spyware at home, improve information-sharing with industry and civil society, and galvanize allies to adopt similar safeguards.

Digital activism, civil society advocacy, and independent judiciaries drove real-world improvements for human rights online during the coverage period.

Georgian people mobilized in March 2023 against a restrictive "foreign agents" bill. (*Zurab Tsertsvadze/AFP via Getty Images*)

Generative AI Supercharges Disinformation

Disinformation campaigns have become a regular feature of the global information space. Over the past 10 years, *Freedom on the Net*'s indicator on content manipulation, which measures the extent to which online sources of information are controlled or distorted by the government or other powerful political actors, has declined more on average than any other indicator in the report.

These campaigns have long been assisted by AI technology for distributing content: automated "bot" accounts on social media have smeared activists into silence and propagated false narratives about electoral fraud to voters, while platform algorithms have promoted untrustworthy and incendiary information over reliable sources.

However, much of the work is still done by humans. During the coverage period, at least 47 countries featured progovernment commentators who used deceitful or covert tactics to manipulate online information, double the number from a decade ago. An entire market of for-hire services has

GLOSSARY OF AI TERMS

Artificial intelligence: A field of computer science in which people build computer programs known as "models" that analyze massive datasets in order to predict, interpret, classify, and generate information.

Machine learning: A subfield of artificial intelligence in which computers learn without a human having to program exact instructions. Machine learning models are "trained" (meaning, developed) to learn patterns based on analysis of large sets of data.

Deep learning: A subfield of machine learning that involves models learning in layers, building simpler patterns into more complex ones. This approach has enabled many recent AI advances, such as recognizing objects in images.

Training data: Data—spreadsheets, text, images, audio, or video recordings—that people use to train machine learning or deep learning models.

Generative AI: Deep learning models that specialize in generating content, including images, text, video, and audio, in response to a specific query or prompt.

Large language model (LLM): A deep learning model trained on vast datasets of text, with the capacity to generate sophisticated and realistic text outputs. Examples include OpenAI's GPT-4, Meta's LLaMA, and Anthropic's Claude.

Computer vision models: A deep learning model trained on vast datasets of images, with the capacity to generate sophisticated and realistic image outputs. Examples include Midjourney and OpenAI's DALL-E.

AI chatbots: Programs that employ AI to understand text-based prompts and generate responses to those prompts. Chatbots built on LLMs include OpenAI's ChatGPT and Google's Bard.

Bots: Automated programs that perform prescribed tasks, often with greater speed and at a larger scale than their human counterparts.

Synthetic media: Images, video, or audio content generated by AI—usually by LLMs, computer vision models, and deep learning–based audio models.

Deepfakes: Photo, video, or audio content that has been created or manipulated (usually via AI) to convincingly portray actions or events that did not in fact occur.

emerged to support state-backed content manipulation. Outsourcing in this way provides the government with plausible deniability and makes attribution of influence operations more challenging. It also allows political actors to reach new and more niche audiences by drawing on private-sector innovation and expertise.

In the coming years, these networks of progovernment human commentators and related companies will undoubtedly increase their reliance on AI-based tools that can create text, audio, images, and video en masse. The affordability, ease of use, and accessibility of consumer-facing generative AI technology have lowered the barrier of entry to the disinformation market. Those with the financial or political incentives will have the capacity to create false and misleading information with these tools, and then leverage existing networks to distribute it at scale. As a result, the information space will grow more diluted and polluted with fabrications, further damaging the internet's role as a source of reliable and diverse content.

Outsourcing to shadowy firms and influencers

State officials have cultivated networks of private actors willing to spread false and misleading content. Rather than taking the political risk or developing the resources to engage in such activity themselves, an electoral campaign, politician, or ministry can simply hire a social media influencer or public relations firm that prioritizes lucrative contracts and political connections over ethical or legal probity.

The Russian private sector has played an ongoing role in spreading disinformation about the Kremlin's full-scale invasion of Ukraine last year. A sprawling and sophisticated operation known as "Doppelgänger" mimicked German, American, Italian, British, and French media outlets to disseminate false and conspiratorial narratives about European sanctions and Ukrainian refugees, among other topics. Doppelgänger has been linked to a loose group of companies and nonprofits with close ties to Russian authorities. Cyber Front Z, another Russian network, relied on Telegram to task commentators with sharing hundreds of posts a day on other platforms that attack critics of President Vladimir Putin and promote anti-Ukraine propaganda.

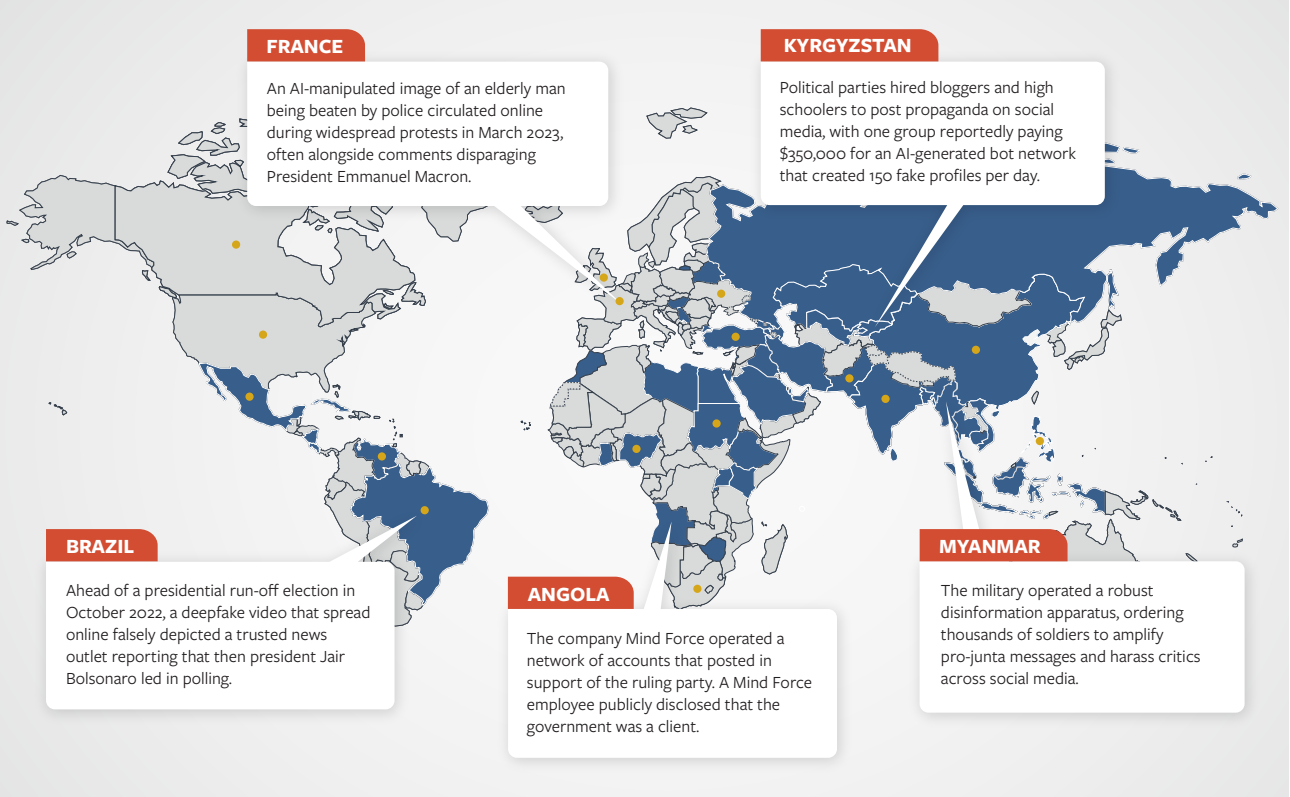
> An entire market of for-hire services has emerged to support state-backed content manipulation.

Israel is home to a growing market of disinformation-for-hire companies. A 2023 investigation by Forbidden Stories, the *Guardian*, and *Haaretz* uncovered the work of an Israel-based firm known as Team Jorge, which reportedly uses an online platform that can automatically create text based on keywords and then mobilize a network of fake social media accounts to promote it. The firm, for instance, disseminated narratives meant to cast doubt on serious allegations that the former director of Mexico's criminal investigations unit was involved in torture, kidnapping, and falsifying evidence. Similarly in August 2022, Meta linked the Israel-based company Mind Force to a network of accounts active in Angola. They primarily posted in support of the ruling Popular Movement for the Liberation of Angola and against the country's main opposition party, and a Mind Force employee publicly disclosed that the Angolan government was a client.

Political actors have also worked to exploit the loyalty and trust that ostensibly nonpolitical influencers have cultivated among their social media followers. Ahead of Nigeria's February 2023 election, influencers were paid—with one reportedly receiving up to $45,000—to spread false narratives linking political candidates with militant or separatist groups. During Kenya's August 2022 election, influencers gamed social media platforms' trending functions to boost misleading political hashtags. For instance, the hashtag #ChebukatiCannotBeTrusted sought to undermine the country's independent electoral authority by suggesting that its leader supported one presidential candidate over the others. Similar networks of influencers were found to have coordinated disinformation campaigns against Kenyan journalists, judges, and members of civil society.

HARNESSING AI TO AUGMENT DISINFORMATION CAMPAIGNS

Governments have long employed human commentators—whether state officials, hired contractors, or party loyalists—to covertly manipulate information online. Generative AI technology is slowly beginning to enhance such distortion campaigns.



47 countries in which progovernment commentators manipulate online discussions

16 countries in which AI-based tools that can generate images, text, or audio were used to distort information on political or social issues

Creating deepfakes to sow doubt, discredit opponents, and manufacture public support

The growing use of generative AI is likely to compound the impact that these existing networks of progovernment commentators have on information integrity and healthy public debate. During the coverage period, AI-based tools that can generate images, text, or audio were utilized in at least 16 countries to distort information on political or social issues. It takes time for governments and the private actors they employ to incorporate new technology into content manipulation, and the early dominance of English-language tools may slow adoption of generative AI technology globally. But this tally of countries is also likely an undercount. Researchers, journalists, and fact-checkers have difficulty verifying whether content is generated by AI, in part because many of the companies involved do not require labeling. Similar obstacles can impede attribution of AI-backed manipulation to a specific creator.

Electoral periods and moments of political crisis served as flashpoints for AI-generated content. In May 2023, amid an escalating political conflict in Pakistan between former prime minister Imran Khan and the military-backed establishment, Khan shared an AI-generated video to depict a woman fearlessly facing riot police. In doing so, he sought to boost a narrative that the women of Pakistan stood by him, not the country's immensely powerful military. During the February 2023 Nigerian elections, an AI-manipulated

A computer displays a broadcast from House of News Español, a nonexistent news channel created by the company Synthesia. The broadcast featured an AI-generated avatar and presented progovernment coverage of Venezuela's economy. (*Freedom House*)

audio clip spread on social media, purportedly implicating an opposition presidential candidate in plans to rig balloting. The content threatened to inflame both partisan animosity and long-standing doubts about the integrity of the electoral system.

AI-manipulated content was also used to smear electoral opponents in the United States. Accounts affiliated with the campaigns of former president Donald Trump and Florida governor Ron DeSantis, both seeking the Republican Party's nomination for the 2024 presidential election, shared videos with AI-generated content to undermine each other's candidacy. One video included three fabricated images of Trump embracing Dr. Anthony Fauci, who led the federal government's COVID-19 response and remains deeply unpopular among critics of pandemic mitigation measures. By placing the fabricated images alongside three genuine photos, the video muddied the distinction between fact and fiction for Republican primary voters. Similarly, in February 2023, a manipulated video that depicted President Biden making transphobic comments spread rapidly across social media. It was presumably created to discredit Biden among voters who support the rights of transgender Americans, which have been under attack in large parts of the country.

AI companies are already being enlisted for state-linked disinformation campaigns. In early 2023, Venezuelan state media outlets used social media to distribute videos produced by Synthesia that depicted news anchors from a nonexistent international English-language channel spreading progovernment messages. Synthesia generates synthetic media for its clients by combining a machine-learning algorithm with videos of paid actors. The research firm Graphika has also linked the company to a campaign to spread pro-CCP disinformation via the nonexistent news station Wolf News to audiences in the United States, though the videos in question were of poor quality and did not achieve significant reach.

During the February 2023 Nigerian elections, an AI-manipulated audio clip spread on social media, purportedly implicating an opposition presidential candidate in plans to rig balloting.

These uses of deepfakes are consistent with the ways in which unscrupulous political actors have long employed manipulated news content and social media bots to spread false or misleading information. Generative AI tools will continue to build on such older tactics, but they may never replace them entirely. During Turkey's elections, a vast progovernment media ecosystem and armies of Twitter bots bombarded the information space with content favoring President Erdoğan and the AKP. One widely circulated video consisted of clips spliced together to falsely depict an outlawed Kurdish militant group supporting opposition presidential candidate Kemal Kılıçdaroğlu. Erdoğan touted the video as substantially true despite appearing to acknowledge that it may have been doctored. The incident underscored how fabricated content can skew an information space even when it is known to be inauthentic. The growing use and sophistication of generative AI will make such videos seem more realistic and thus more challenging to debunk in the future.

The consequences of AI-generated disinformation campaigns

Even if deepfakes are obviously fabricated or quickly exposed as such, they still contribute to a decaying information space. They can undermine public trust in democratic processes, incentivize activists and journalists to self-censor, and drown out reliable and independent reporting. AI-generated imagery that sensationalizes outrage on divisive topics can also entrench polarization and other existing tensions within society. In extreme cases, it could galvanize violence against individuals or whole communities. The impact of AI-generated disinformation will deepen as the quality and quantity of the technology's output continues to exceed the capacity of observers, moderators, or regulators to detect, debunk, or remove it.

Like digital repression more broadly, AI-generated disinformation campaigns disproportionately victimize and vilify segments of society that are already under threat. The overwhelming majority of nonconsensual deepfakes featuring sexual imagery target women, often with the aim of damaging their reputations and driving them out of the public sphere. An online campaign using AI-manipulated pornographic videos was used to discredit prominent Indian journalist and government critic Rana Ayyub as early as 2018. During the coverage period, Nina Jankowicz, a US expert on disinformation, was subjected to pornographic deepfakes as part of a broader campaign against her and her work. These uses of sexualized deepfakes represent a twisted evolution of a much older practice, the nonconsensual distribution of intimate images of women activists. For example, during the coverage period, a smear campaign that featured nonconsensual intimate imagery of Azerbaijani prodemocracy activists and opposition figures spread across Telegram, TikTok, Facebook, and progovernment news sites.

The growing use of AI-generated false and misleading information is exacerbating the challenge of the so-called liar's dividend, in which widespread wariness of falsehoods on a given topic can muddy the waters to the extent that people disbelieve true statements. For example, political actors have labeled reliable reporting as AI-enabled fakery, or spread manipulated content to sow doubt about very similar genuine content. In April 2023, the Indian state of Tamil Nadu was rattled by a political controversy after leaked recordings captured Palanivel Thiagarajan, a prominent official in the state's ruling Dravida Munnetra Kazhagam party, disparaging his colleagues. Thiagarajan denounced the audio clips as machine generated; independent researchers determined that at least one was authentic. In Ethiopia, after a member of the ruling Prosperity Party was killed in the Amhara region in April 2023, state-affiliated media outlets released audio that purportedly linked a militia group to the killing. An organization released a report alleging that the audio recordings were manipulated using AI; another fact-checking group then accused the organization of being fake, casting doubt on the claim of AI manipulation.

Companies like OpenAI and Google have imposed guardrails to reduce some overtly harmful uses of their chatbots. But researchers have identified techniques to break through popular chatbots' safeguards so that they generate harmful, false, discriminatory, or abusive text, including misinformation about the COVID-19 pandemic and statements that mirror Russian propaganda about the invasion of Ukraine. Generative AI applications have also produced false and harmful statements about prominent members of civil society. The dangers of AI-assisted disinformation campaigns will skyrocket as malicious actors develop additional ways to bypass safeguards and exploit open-source models, and as other companies release competing applications with fewer protections in place.

Governments Harness AI to Reinforce Censorship

Advances in generative AI may prove a double-edged sword for authoritarian governments. Today's popular chatbots could provide people in closed environments with indirect access to uncensored information sources, echoing the early promise of news websites and social media. But some of the most authoritarian regimes are already responding to this potential with new restrictions. The history of internet governance suggests that more states will quickly adapt their legal frameworks and technical mechanisms to control how their citizens interact with these emerging digital products.

As some governments are moving to restrict access to generative AI or control its outputs, many are also forcing companies to use AI to remove content from their platforms at a speed and scale that would be impossible for human censors or less sophisticated technical methods. These censorship requirements tend to concentrate on content that is deemed illegal under local law—a category that, in many countries, includes expression on political, social, or religious topics that should be protected under international human rights standards. Innovations in the AI field have allowed governments to carry out more precise censorship that is less detectable, minimizing public backlash and reducing the political cost to those in power.

While AI has allowed for more subtle and efficient forms of content removal, blunt censorship remains pervasive. Shutdowns of internet service and blocks on entire social media platforms continued to be key tactics of information control around the world. The number of countries where governments imposed outright blocking on websites that hosted political, social, and religious speech reached an unprecedented high of 41 this year. Democracies are not immune to this trend. States that have long been defenders of internet freedom imposed censorship or flirted with proposals to do so, an unhelpful response to genuine threats of foreign interference, disinformation, and harassment.

Innovations in the AI field have allowed governments to carry out more precise censorship that is less detectable, minimizing public backlash and reducing the political cost to those in power.

Generative AI draws authoritarian attention

This coverage period's newly launched text-based generative AI applications like ChatGPT and Bard may allow users to sidestep government censorship, because the systems are trained on data from the global internet, including information that is typically suppressed in authoritarian states. The most technically sophisticated authoritarian regimes grappled with this risk, and some attempted to restrict access to the new chatbots. In February 2023, Chinese regulators ordered tech conglomerates Tencent and Ant Group to ensure that ChatGPT is not integrated into or accessible via their services, including through the third-party apps on their app stores. Apple removed over 100 ChatGPT-like apps from its Chinese app store to comply with local rules. Similarly, Vietnamese officials warned citizens against using ChatGPT, asserting that it "distorts," smears, and opposes the state and the ruling Communist Party of Vietnam (CPV).

Early research indicates that chatbots' outputs reflect the censorship embedded in their training data, a reminder that generative AI tools influenced by state-controlled information sources could serve as force multipliers for censorship. Developers in some repressive countries have moved to create their own chatbots. For instance, several Russian companies—including Yandex and Sistemma—have

Chatbots produced by China-based companies have refused to engage with user prompts on sensitive subjects like Tiananmen Square.

launched such products. The Chinese government has sought to regulate training data directly: Chinese consumer-facing generative AI products, like Baidu's ERNIE Bot and Alibaba's Tongyi Qianwen, are required to implement stringent content controls and ensure the "truth, accuracy, objectivity, and diversity" of training data, as defined by the CCP. Indeed, chatbots produced by China-based companies have refused to engage with user prompts on sensitive subjects like Tiananmen Square and have parroted CCP claims about Taiwan.

Emerging state attempts to control chatbots mirror previous efforts to restrict new social media platforms, with the world's most technically sophisticated authoritarian governments leading the charge. As generative AI-based tools become more accessible and widely used, a growing number of governments will focus on ensuring that they reinforce rather than challenge existing information controls.

Ordering platforms to use AI for censorship

In at least 22 countries, social media companies were required—either explicitly or indirectly through the imposition of tight deadlines for the removal of banned material—to use automated systems for content moderation. While such systems are used by social media platforms around the world, the laws in many countries prohibit forms of political, social, and religious speech that should be protected under international human rights standards. By obliging platforms to use machine learning to comply with censorship rules, governments are effectively forcing them to detect and remove banned speech more efficiently. This use of AI also masks the role of the state in censorship and may ease the so-called digital dictator's dilemma, in which undemocratic leaders must weigh the benefits of imposing online controls against the costs of public anger at such restrictions.

Students in Kolkata hosted a film screening in January 2023 for a documentary about Indian prime minister Narendra Modi. Indian authorities had previously ordered YouTube and Twitter to block the documentary from being viewed within the country. (*Dipayan Bose/SOPA Images/LightRocket via Getty Images*)

Indian prime minister Narendra Modi and his Hindu nationalist Bharatiya Janata Party have incorporated censorship, including the use of automated systems, into the country's legal framework. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules require large social media platforms to use AI-based moderation tools for broadly defined types of content—such as speech that could undermine public order, decency, morality, or the country's sovereignty, integrity, and security, or content that officials had previously ordered removed. For instance, in early 2023, authorities ordered YouTube and Twitter to restrict access within India to a British Broadcasting Corporation documentary about communal violence during Modi's tenure as chief minister of the state of Gujarat. Because the government ordered the restriction of the documentary, the IT Rules require the two platforms to use automated scanning tools to sweep up any additional posts that share the film. As the country prepares for general elections in 2024, the government's expanding censorship regime is creating an uneven playing field by silencing criticism of and independent reporting on the ruling party.

In more authoritarian contexts, automated censorship systems could close what little space remains for online expression. The Vietnamese government imposes tight controls on digital platforms to curb dissent, independent reporting, and other forms of political and social speech. For example, authorities have reportedly compelled Meta to remove all criticism of specified CPV officials. Regulations passed in August 2022 empower the Ministry of Public Security to block platforms that do not comply with a requirement to remove "toxic" content within one day of being notified, a threat that incentivizes overbroad removal at a pace only achievable through automation. Authorities have since explicitly demanded that companies use AI to remove so-called toxic content.

In more authoritarian contexts, automated censorship systems could close what little space remains for online expression.

Such measures are growing in popularity among governments with less robust technological and regulatory capacity. In Nigeria, where authorities have imposed significantly less censorship than their counterparts in Vietnam and India, a code of practice introduced in October 2022 requires companies to remove content within 48 hours of notification from a government agency. The code was introduced after then president Muhammadu Buhari imposed a seven-month block on Twitter because the company removed a post in which he appeared to threaten violence against separatists. It is unclear to what extent the code has been enforced since the election of President Bola Tinubu in February 2023.

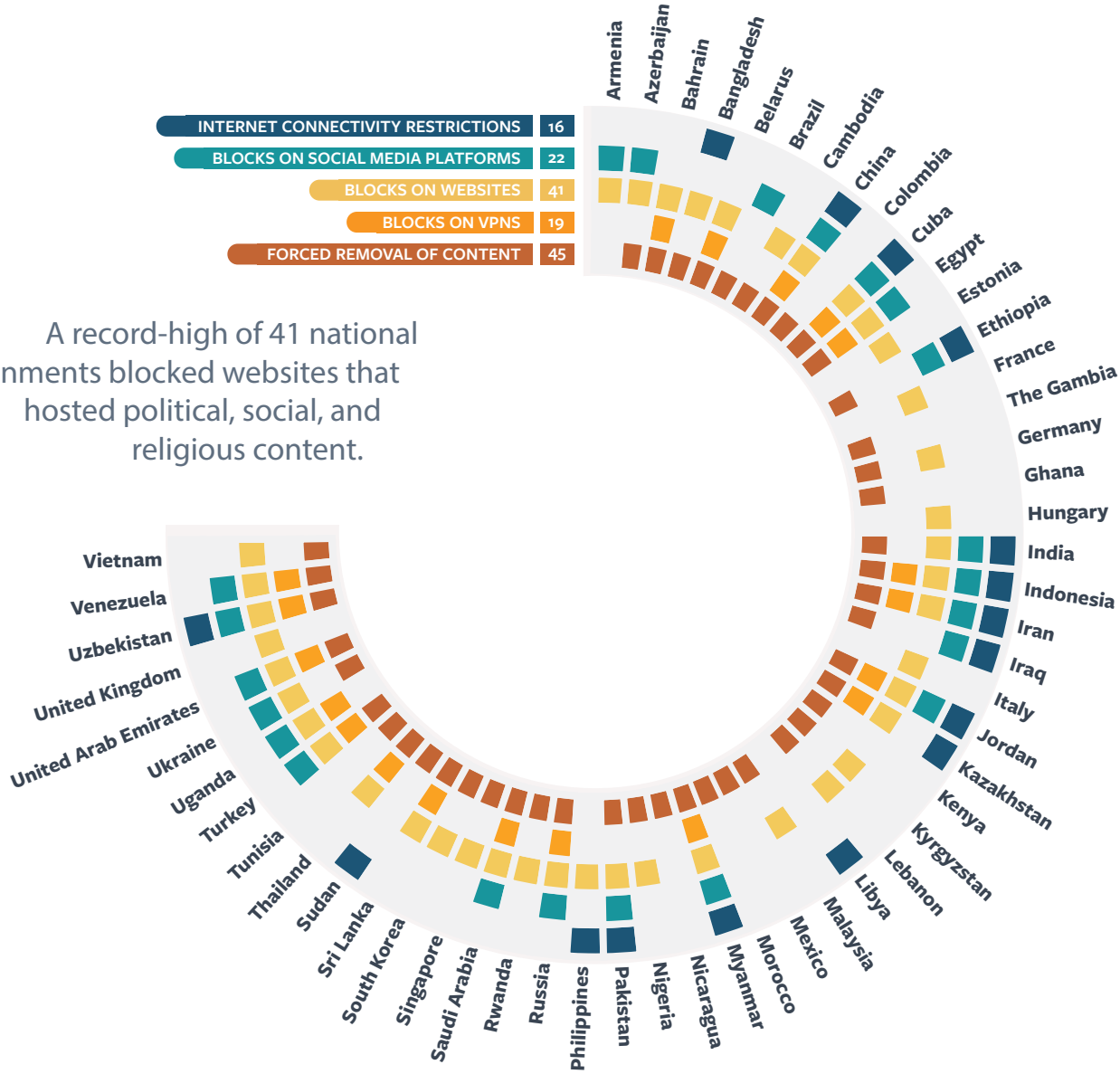
Automated systems play a positive and supportive role in conducting content moderation at scale, including by detecting influence operations and reviewing dangerous and harmful content—such as child sexual abuse imagery and depictions of graphic violence—that traumatizes human moderators. However, even when these systems are used appropriately, they can excessively or inconsistently flag online material, especially content in languages other than English or in slang, thus increasing the likelihood that political, social, and religious speech will be removed. To protect against that risk and to ensure that the systems strengthen information integrity, laws covering online content and AI should be grounded in human rights principles, require audits and increased transparency regarding the use and impact of algorithms, and include mechanisms for notice, explanation, redress, and appeal.

Conventional forms of censorship endure

Especially during times of crisis or protests, AI-powered moderation and filtering tools may struggle to keep up with a surge of unexpected content and expressions of dissent. Blunter forms of censorship will thus continue to be utilized. During the coverage period, internet connectivity was restricted in at least 16 countries. One of them was Iran, where the regime's technically advanced censorship apparatus was overwhelmed by mass mobilization in 2022 and 2023, forcing authorities to cut off service. Sudanese authorities similarly restricted access to the internet in April 2023, severing critical communication channels at a time when hundreds of thousands of people were caught in the middle of heavy combat between rival paramilitary and military forces.

TRIED AND TRUE: CONVENTIONAL CENSORSHIP METHODS PROLIFERATE

Traditional forms of online censorship surged during the coverage period, utilized by governments from across the democratic spectrum.



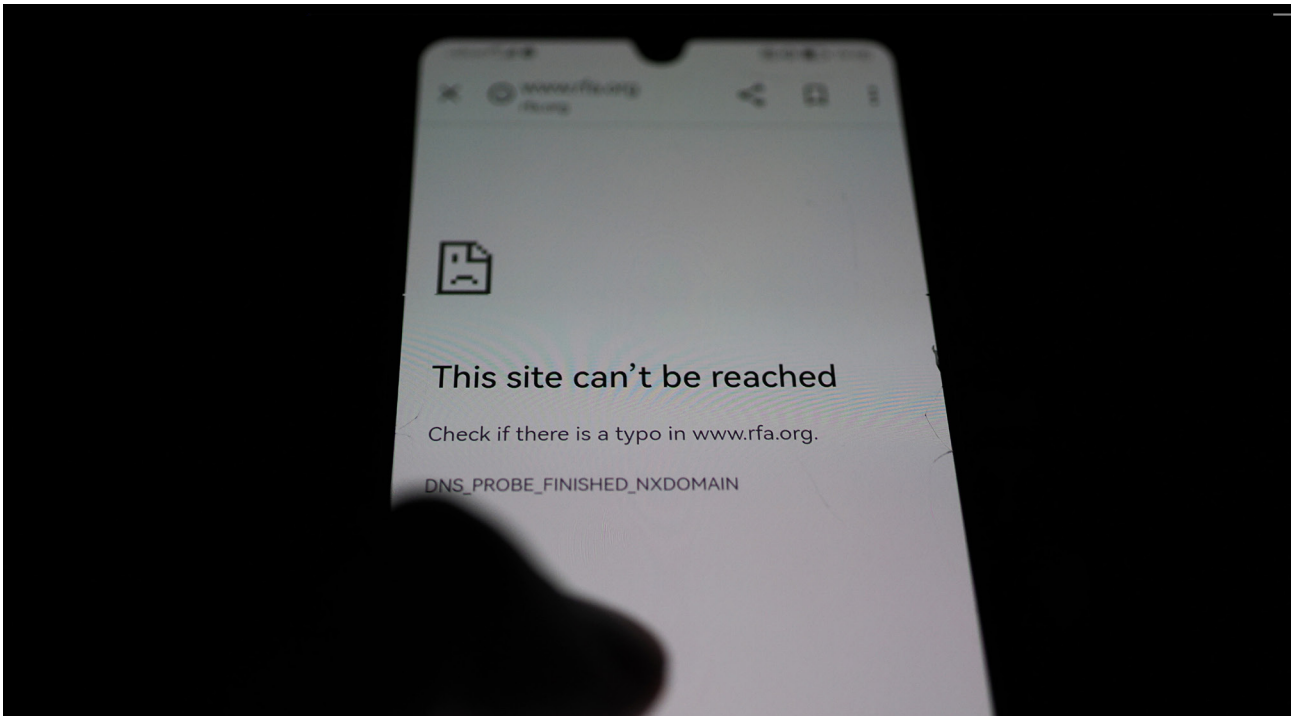
Of the 70 countries covered by *Freedom on the Net*, governments in a record-high 41 blocked websites that hosted political, social, and religious speech. Roskomnadzor, Russia's media and telecommunications regulator, requires internet service providers to install a unique, government-produced deep packet inspection (DPI) system that enables the blocking of websites across the country. The Kremlin has used this system to block global social media platforms, Ukrainian news sites, and domestic sites that carry any hint of dissent regarding its invasion of Ukraine. The coverage period also featured increased Russian blocking of websites that host LGBT+ content, part of a broader assault on that community in the country. The Belarusian government, which has aided Moscow's military aggression, has blocked more than 9,000 websites, including a slew of independent news sites and associated mirror sites that are maintained by Belarusian journalists working in exile.

Governments are increasingly blocking digital platforms as a means of compelling them to comply with internet regulations. Indonesian authorities restricted access to Yahoo, the gaming platform Steam, payment processor PayPal, and several other sites in July and August 2022 in order to force compliance with Ministerial Regulation 5, which requires the removal of overly broad categories of prohibited speech under tight deadlines. In Brazil in April 2023, after Telegram failed to hand over user data related to neo-Nazi chat groups, a judge ruled that the platform had violated data retention requirements and ordered it blocked entirely. Another judge reversed the ban days later, imposing a more proportionate daily fine on the company and finding that the wholesale blocking was too broad and unreasonably restrictive.

Concerningly, some democratic governments that have traditionally defended freedom of expression considered or imposed censorship during the coverage period, often citing concerns about foreign interference, fraud, and online safety. A French bill presented in May 2023 would require browsers, not internet service providers, to block websites when so instructed by an administrative body, as opposed to a judicial order. The draft law would force browser developers like Mozilla to create a new technical process for blocking, which could be exploited in France and around the world. A month later, concerns about overly broad censorship arose again when President Emmanuel Macron suggested the possibility of blocking or banning Snapchat, TikTok, and other services used by younger populations amid protests and related violence that followed the police killing of a teenager of Algerian descent. Although no such restrictions were implemented, a democratic leader's rhetorical endorsement of social media blocks as an appropriate response to protests could help to legitimize this form of censorship globally.

A democratic leader's rhetorical endorsement of social media blocks as an appropriate response to protests could help to legitimize this form of censorship globally.

Across the Atlantic, some politicians and state-level governments in the United States pushed for an outright



Ahead of the voting in Cambodia's July 2023 election, authorities blocked access to several independent news outlets, including Radio Free Asia. (*Satoshi Takahashi/LightRocket via Getty Images*)

ban on TikTok, owned by the Chinese tech company ByteDance, citing potential threats to national security and the risk that the Chinese government could access Americans' personal data. Montana became the first state to enact a law that, beginning in January 2024, forces companies like Apple and Google to prevent Montanans from downloading TikTok from their respective app stores. Since it was adopted in May 2023, the law has faced constitutional challenges. At the federal level, meanwhile, proposed bills would provide President Biden with the legal authority to ban TikTok nationwide. While the platform's ownership by ByteDance raises serious human rights and national security concerns, a ban would undermine the constitutional right to free speech for millions of Americans, and would almost certainly encourage other governments to limit access to specific social media platforms. Such a ban would also fail to address the underlying threats posed by TikTok, the tech sector's broader data-collection ecosystem, and the multiple ways in which foreign governments and nonstate actors can access and exploit Americans' information. A more comprehensive, effective, and rights-respecting approach to these problems would include stronger regulatory oversight and new legislation to improve privacy protections, require platform transparency and risk assessments, and guard against weak data security practices.

Regulating AI to Protect Internet Freedom

Many of the debates surrounding AI have their roots in long-standing policy questions related to internet governance: How can regulation effectively protect people from malicious state and nonstate actors, while fostering a competitive and innovative private sector? What legal responsibilities should companies bear when they fail to prevent their products from being used in harmful ways? The lessons learned from the past decade of deliberations regarding government oversight, the need for robust global civil society engagement, and the problem of overreliance on self-regulation collectively provide a roadmap for this new era. Given the ways in which AI is already contributing to digital repression, a well-designed regulatory framework is urgently necessary to protect human rights in the digital age.

Regulators take aim at AI

Only a limited number of companies currently have the financial and computational resources necessary to develop AI systems using complex large language models. Similarly, few governments have the regulatory capacity and technical literacy to design robust rules governing the rollout of generative AI. While governments across the democratic spectrum, from Indonesia to the United Arab Emirates, have begun launching high-level strategies or frameworks around AI broadly, many have yet to transfer these pronouncements into legislation. As the technology's benefits and harms become more apparent, policymakers may look to early examples from China, the EU, and the United States for guidance on their own legislation.

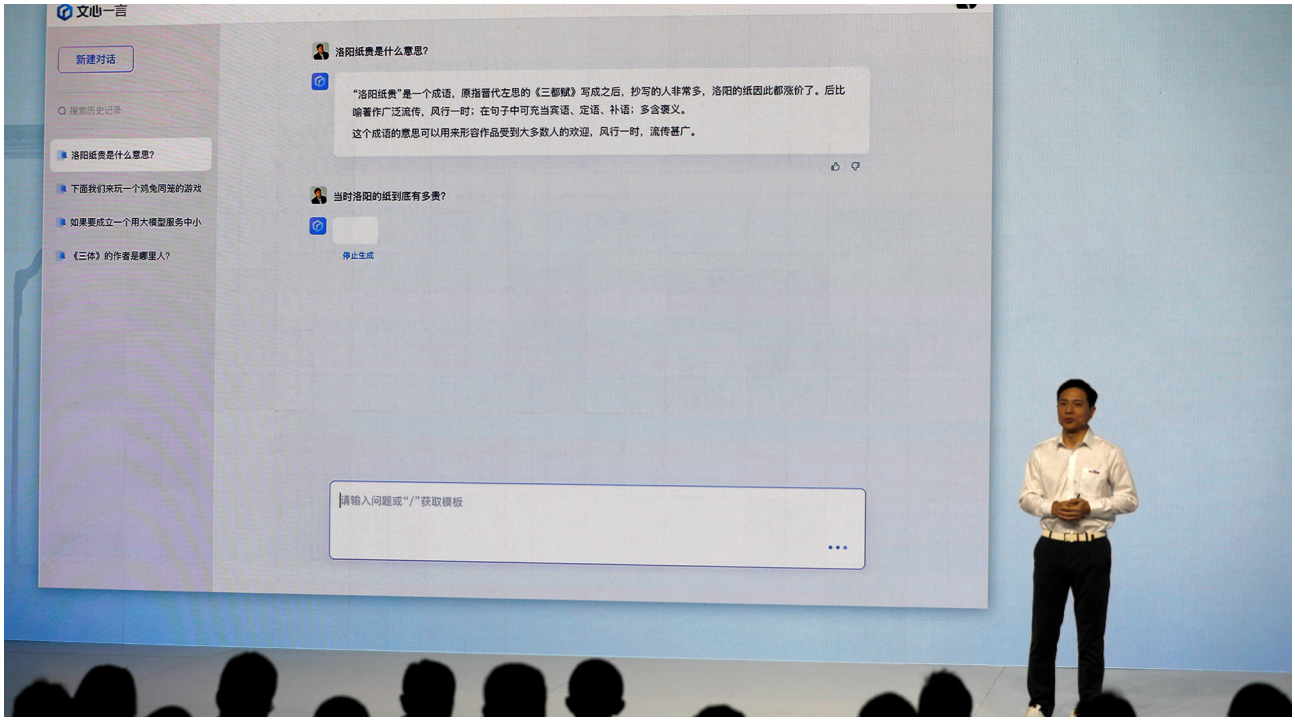
The CCP has invested heavily in the AI industry while ensuring that the companies in question will serve its authoritarian priorities. The Cyberspace Administration of China (CAC), a powerful regulatory body, has embarked on a yearslong effort to integrate CCP censorship goals into the country's content recommendation algorithms, synthetic media, and generative AI tools. For example, the CAC approved 41 suppliers of generative AI services in June 2023, and five chatbots were released to the public in August.

> The lessons learned from the past decade of deliberations on internet governance provide a roadmap for this new era.

Such applications are required to adhere to or promote "core socialist values" and exclude content that is deemed undesirable by the CCP. Similar rules have long been in place for Chinese social media companies.

Since 2021, the EU has developed a sprawling framework that could serve as a global model for AI governance, just as Brussels's General Data Protection Regulation has become a key reference for data protection laws around the world. The draft Artificial Intelligence Act, which was in final negotiations as of August 2023, would tailor obligations based on the level of risk associated with particular technologies, including facial recognition, recommendation algorithms on social media, chatbots, AI tools that can generate images and videos, and the use of AI in political campaigning. AI products that are deemed to present an unacceptable risk would be banned altogether, including social credit systems, predictive policing tools, and certain uses of biometric surveillance. Technologies with a "high" or "limited" risk would be subject to a spate of pre- and post-market requirements, such as registration and increased transparency.

In the United States, the Biden administration began its development of AI governance with a push for industry self-regulation. The Blueprint for an AI Bill of Rights, released in October 2022, laid out a set of principles to guide AI design, use, and deployment. The guidelines include protections against abusive data practices, ineffective and unsafe systems, and algorithmic discrimination, which occurs



Baidu's chief executive showcases ERNIE Bot, the company's AI chatbot, in March 2023. China-based companies like Baidu must implement strict content controls on generative AI products. (*REUTERS/Tingshu Wang*)

when biases embedded in training data are expressed in a program's outputs. The blueprint also calls for companies to offer people a human alternative to automated systems when appropriate, and to inform people when and how such systems are operating. In July 2023, after the coverage period, the administration secured voluntary commitments from Amazon, Anthropic, Google, Inflection, Meta, Microsoft, and OpenAI regarding AI safety and security. While self-regulation is an important starting point, it must be matched with meaningful oversight. Further executive action was anticipated at the time of writing, but to ensure that AI bolsters rather than harms internet freedom, members of Congress should work with civil society and the executive branch to craft bipartisan legislation that takes a rights-based approach to AI governance and transforms guiding principles into binding law.

The EU has developed a sprawling framework that could serve as a global model for AI governance.

A trust and safety deficit diminishes hope for self-regulation

A series of business decisions during the coverage period cast further doubt on the private sector's willingness and capacity to self-regulate. Across a number of major platforms, teams focused on content, integrity, trust, and safety—including those tasked with setting, maintaining, and enforcing rules for user behavior—experienced a dramatic reduction in staff and resources. Some companies also pared back transparency mechanisms as well as content policies that were intended to reduce the spread of false and misleading information. This shift in priorities suggests that companies have forgotten the lessons from past controversies. The industry's deficient investments in content moderation around the world, failure to heed calls for extra care during electoral or other sensitive periods, and inadequate adjustments to products and policies in response to crises have all had the effect of inflaming online and offline violence.

Nowhere was this shrinking and reprioritization of resources more dramatic than at X, formerly known as Twitter, after it was purchased by tech investor and entrepreneur Elon Musk in October 2022. As part of its mass layoffs, the company dismissed experts on trust and safety, human rights, public

policy, and regional issues in Africa, Asia, and Latin America. X also reduced its transparency with the public, for example by putting its application programming interface (API) behind a paywall, scaling back its own transparency reports about state demands, and pausing its reporting to Lumen, a database that publishes government orders for content removal. Economic concerns during the coverage period also led Meta, Amazon's Twitch, Google, Snap, and Microsoft to impose mass layoffs, slashing teams that worked on topics such as elections, AI ethics, or content moderation. Many contractors who carried out content moderation, and who already suffered from inadequate pay and resources, were also let go.

Companies appear to be wagering that they can use AI to make up for the loss of human expertise, even when addressing the problems arising from AI itself. OpenAI has proposed using ChatGPT to moderate online content and develop rules for content moderation. Indeed, the new wave of generative AI tools could be a powerful asset in reviewing content that human reviewers would find distressing. However, human oversight remains critical to ensuring that automated systems and their content removals are

Companies appear to be wagering that they can use AI to make up for the loss of human expertise, even when addressing the problems arising from AI itself.

ENSURING AI ADVANCES INTERNET FREEDOM

The lessons learned from the past decade of deliberations on internet governance provide a roadmap for AI regulation.

not overbroad or discriminatory. Overreliance on large language models for higher-order tasks that require context and nuance, like writing content policy, should be treated with skepticism.

The stakes of this wager are high, especially ahead of 2024 elections in pivotal countries and as AI-generated content grows more prevalent. The firing of regional and legal teams entails a loss of institutional knowledge on political parties, disinformation networks, and regulatory systems. Rolling back content policies intended to provide context for readers will weaken information integrity. And reduced platform transparency will limit civil society's ability to analyze evolving censorship tactics and push for accountability. Ultimately, some companies may choose to further deprioritize policy development and enforcement outside of their perceived core markets. But decisions that maximize short-term profits while accepting negative human rights consequences will in practice create a more dangerous experience online, undermine a service's competitive appeal, and threaten the strong rule-of-law environment on which all businesses depend.

Ensuring that AI advances human rights online

Technology cannot be a substitute for governance. Most AI models are highly opaque, dependent on the processing of billions of datapoints, and effectively under the control of a handful of companies that reveal little about their development and training. Their inscrutable structure is fundamentally at odds with democratic values such as transparency, proportionality, and accountability, and their information inputs are often hotbeds of potential bias. Companies that create or deploy AI systems, from the newest startups to the most established giants, should cultivate an understanding of previous efforts to strengthen platform responsibility, which have produced both successes and failures over the past decade. But given the private sector's natural inclination to focus on profit generation, its AI products require supervision by an informed public, a global group of civil society organizations, and empowered regulators.

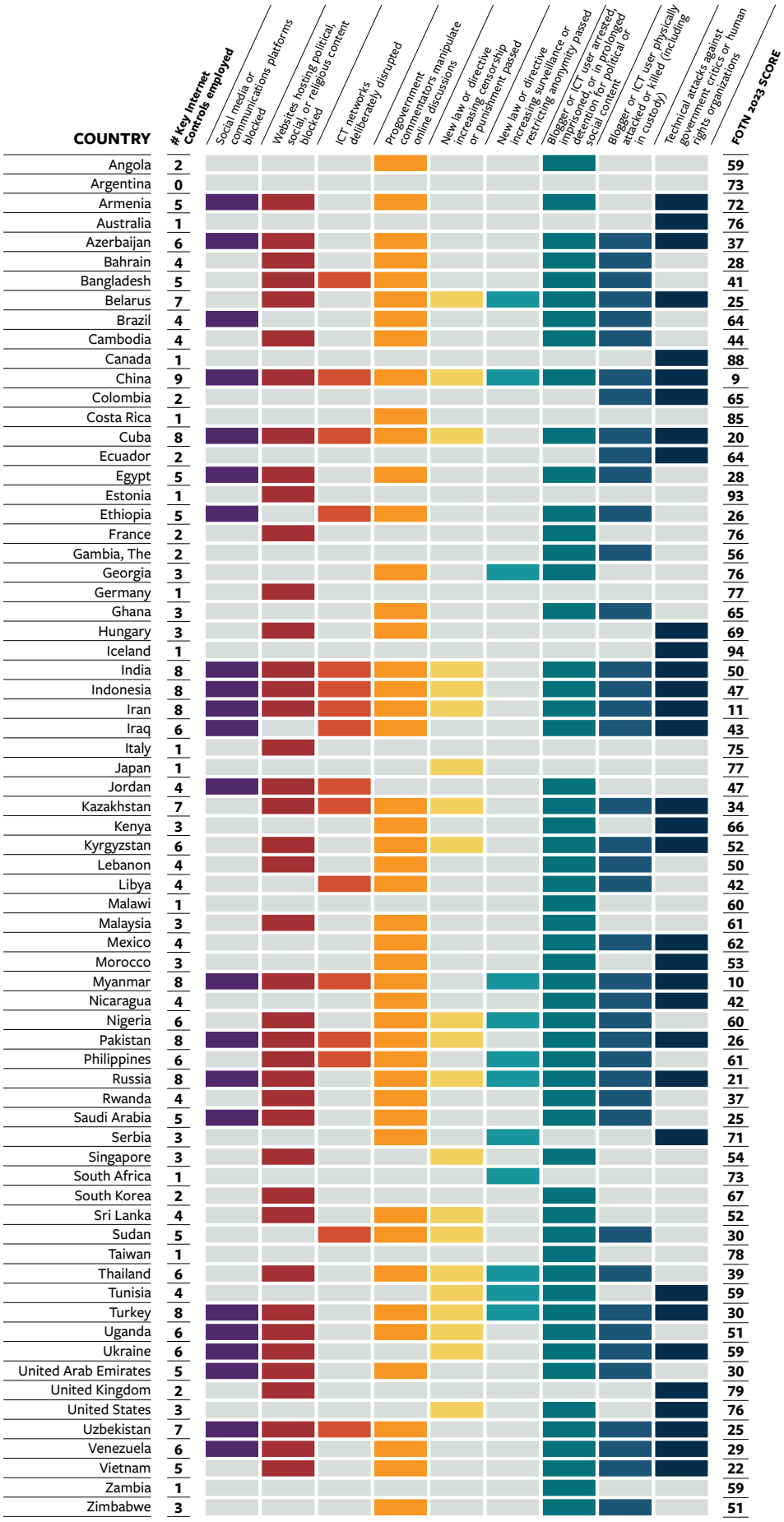
An effective defense of internet freedom requires not just developing AI governance systems, but also addressing long-standing threats to privacy, free expression, and access to information.

Government regulation should be aimed at delivering more transparency, providing effective mechanisms of public oversight, and prioritizing the protection of human rights. When designed and used safely and fairly, AI can help people evade authoritarian censorship, counter false and misleading information, monitor elections to ensure that they are free and credible, and bolster documentation of human rights abuses. To bring about effective and rights-respecting AI governance, civil society should be included from the start. Nonprofit organizations, investigative reporters, and human rights activists have been indispensable players behind past wins for internet freedom. Among other contributions, they can build and sustain public pressure and spur action by legislators, regulators, and the industry.

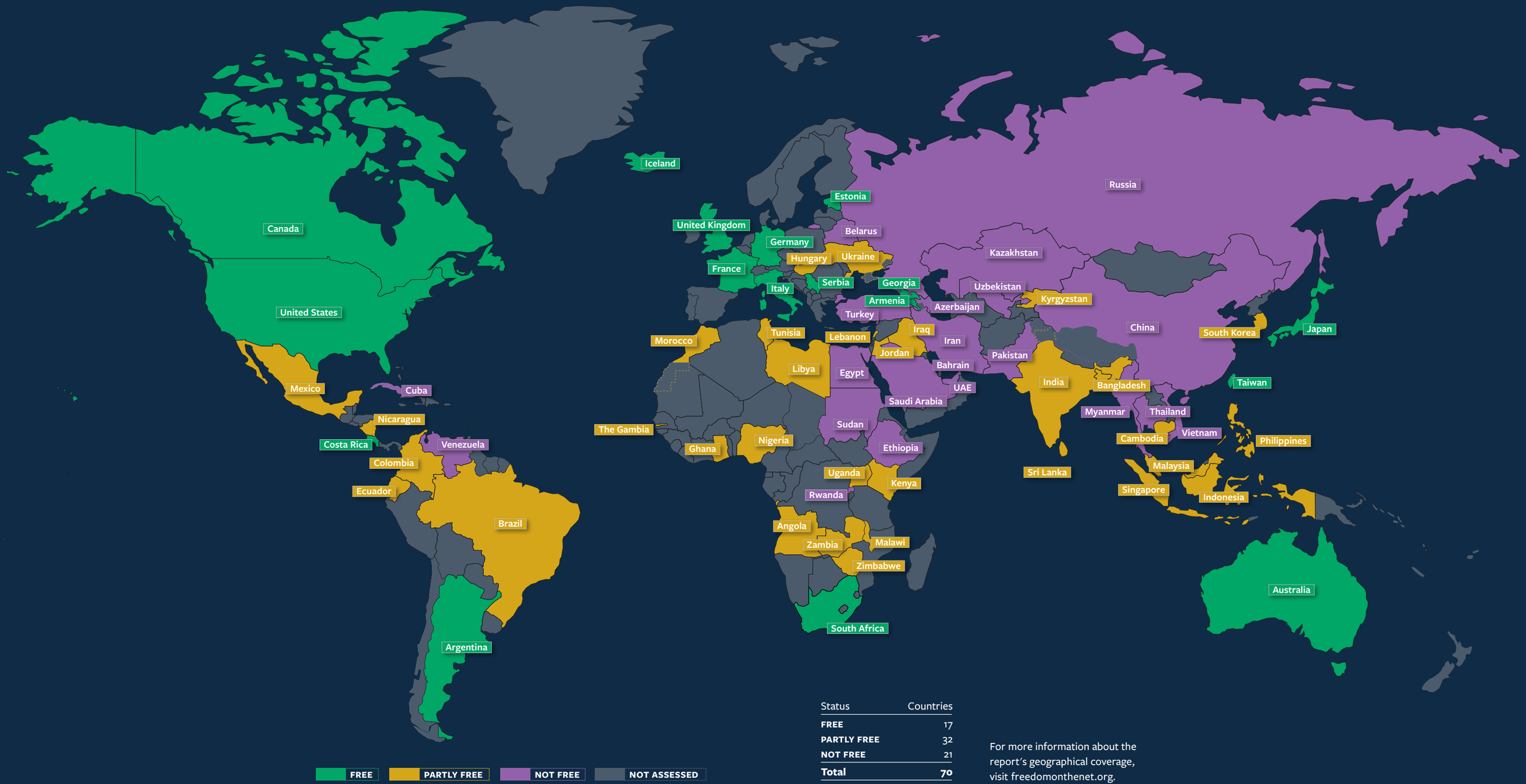
Policymakers and their civic and private-sector partners should take care not to lose momentum in protecting overall internet freedom, especially as AI technology augments the forces driving its multiyear decline. Indeed, to the extent that AI simply exacerbates existing problems associated with digital repression, existing solutions—ensuring that companies minimize the data they collect, reforming legal frameworks for surveillance and censorship, and strengthening information literacy and platform responsibility—should be thoroughly implemented. An effective defense of internet freedom requires not just developing AI governance systems, but also addressing long-standing threats to privacy, free expression, and access to information that have corroded the broader digital environment.

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 2022 to May 2023. The Key Internet Controls reflect restrictions on content of political, social, or religious nature.



FREEDOM ON THE NET 2023

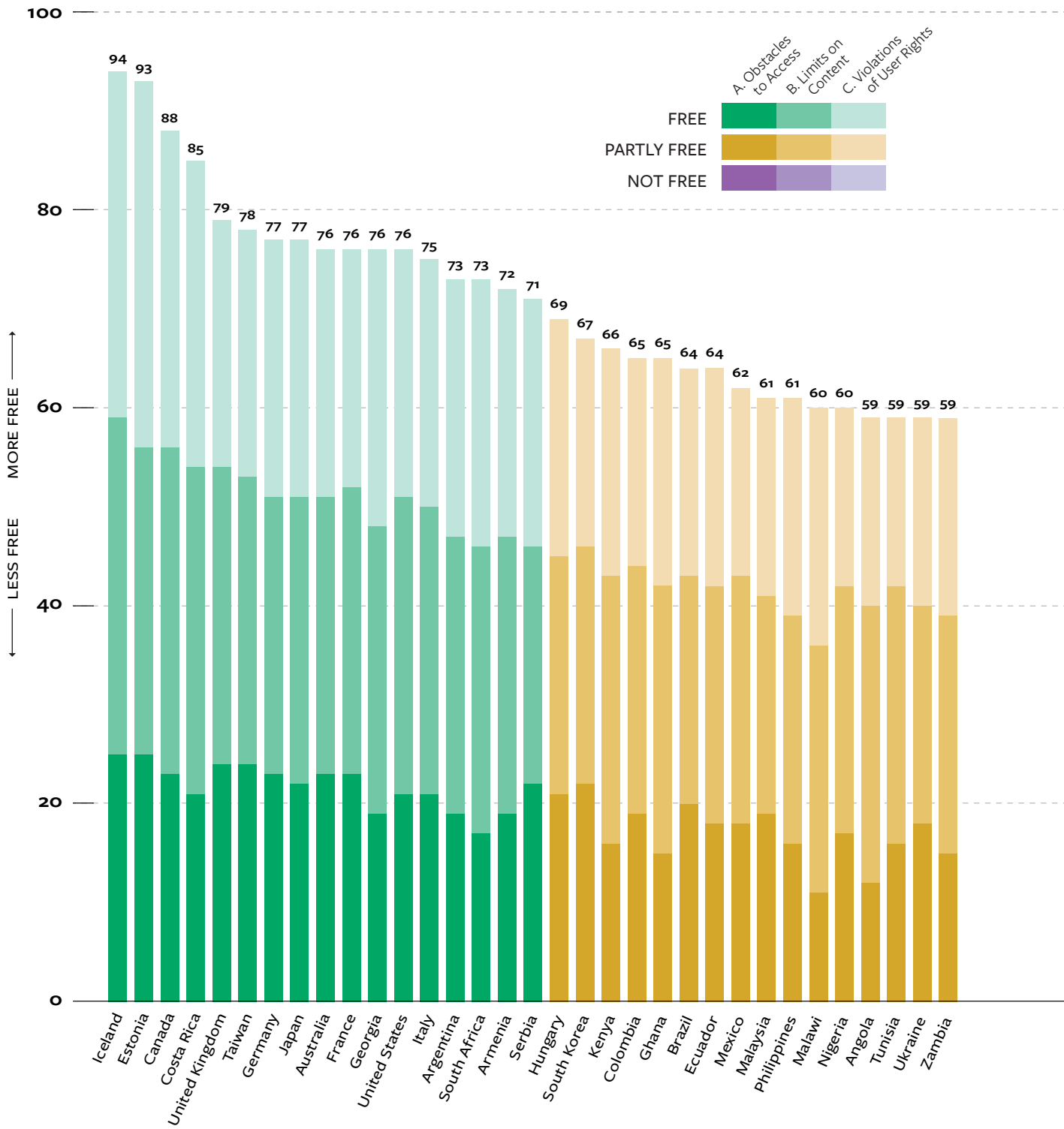


Status	Countries
FREE	17
PARTLY FREE	32
NOT FREE	21
Total	**70**

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

GLOBAL RANKINGS

100 = Most Free 0 = Least Free



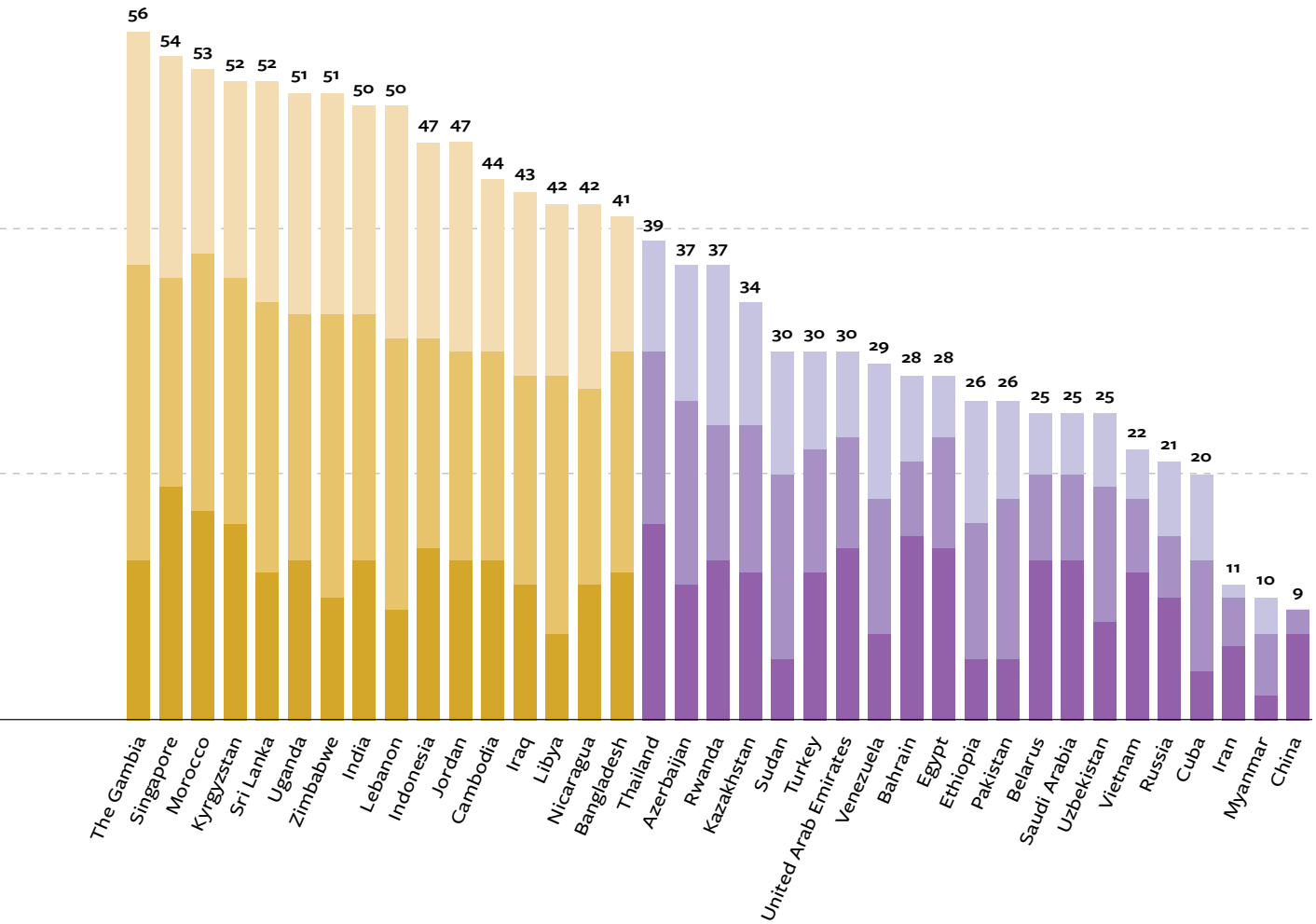
Freedom on the Net 2023 covers 70 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems. Each country receives a numerical score from **100 (the most free)** to **0 (the least free)**, which serves 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.



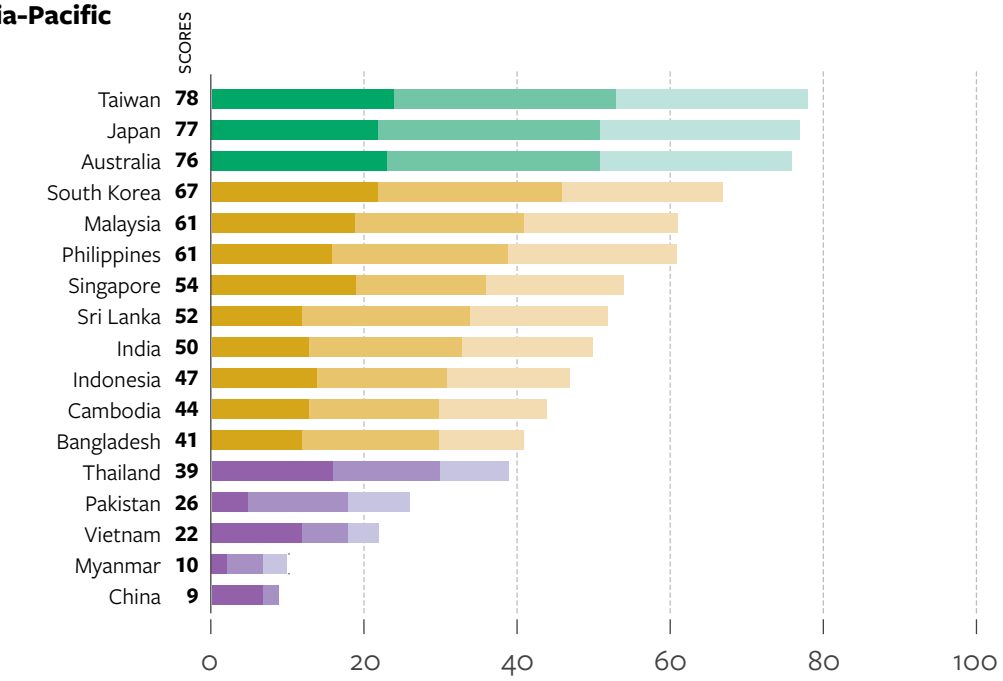
REGIONAL RANKINGS

Freedom on the Net 2023 covers 70 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

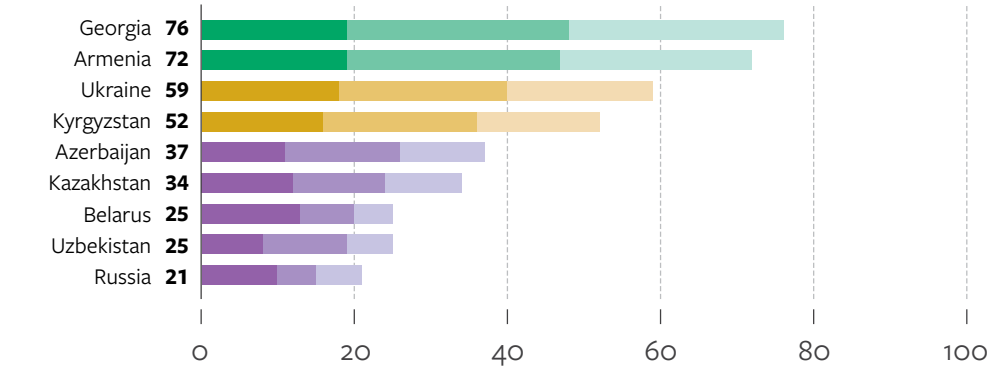
A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights

0 = Least Free
100 = Most Free

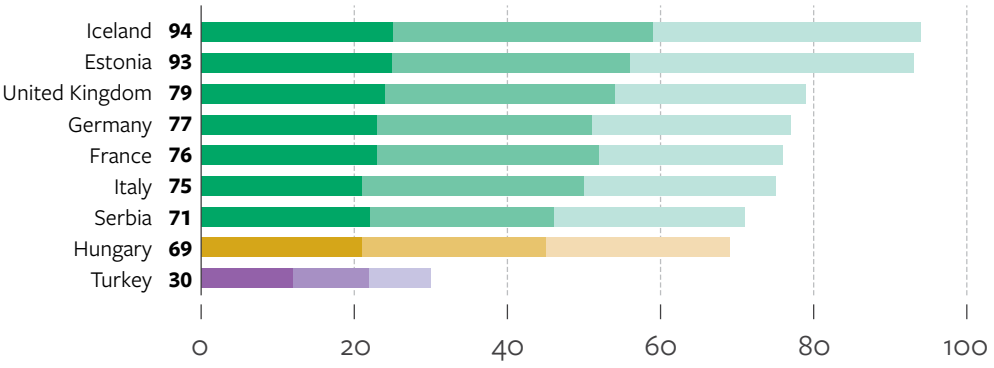
Asia-Pacific



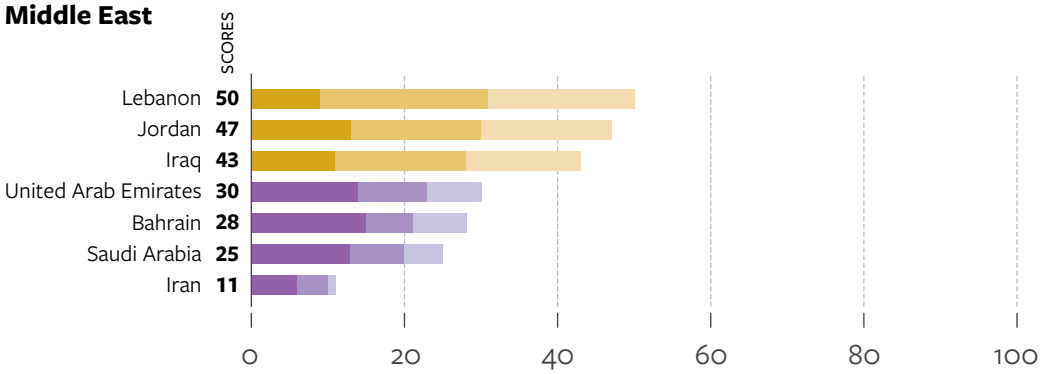
Eurasia



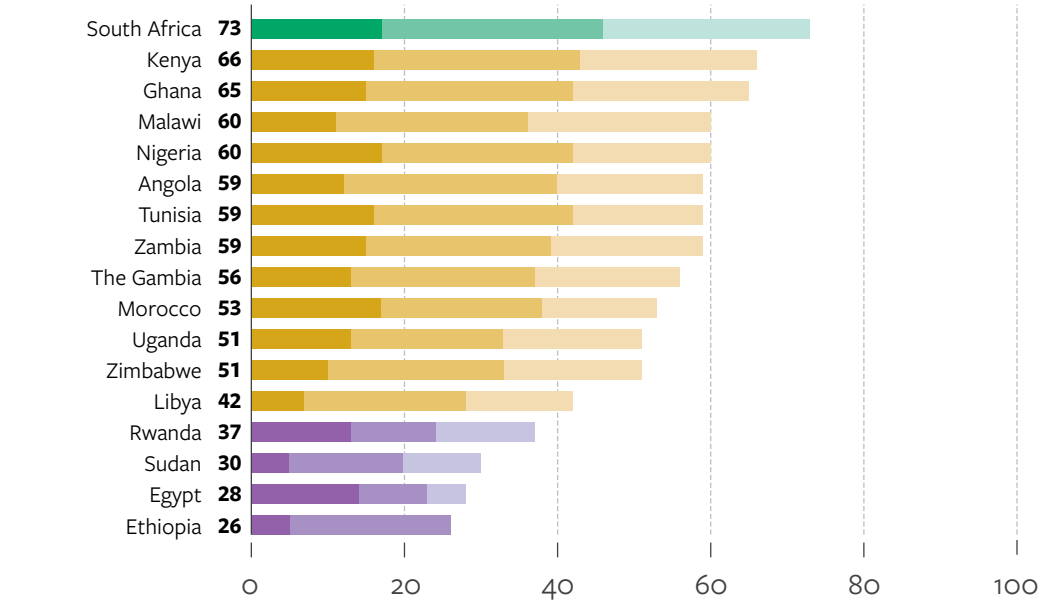
Europe



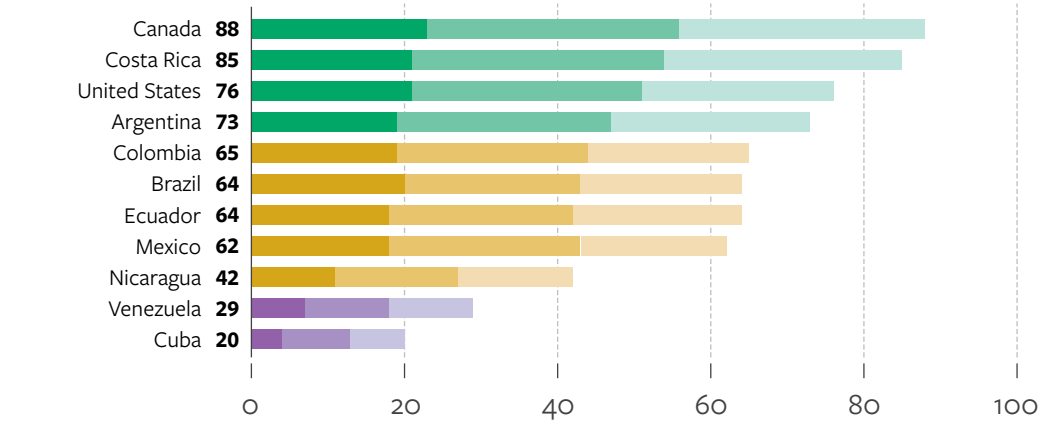
Middle East



Africa



Americas



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, and private companies can adopt to prevent or mitigate illiberal uses of digital technology by both domestic and foreign actors, as well as the broader societal harms that the internet can exacerbate. 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 solutions to address them.

1. PROMOTE FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION

Freedom of expression online is increasingly under attack as governments continue to restrict connectivity and block social media platforms and 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 circumvention 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 social media and messaging 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 transparency, data privacy, and platform responsibility, such as mandatory human rights due diligence and risk assessments.

Legal frameworks addressing online content should establish special obligations for companies tailored to their size and their services, incentivize platforms to improve their own standards, and require human rights due diligence and reporting. Such requirements 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 also provide opportunities for vetted researchers to access platform data—information that can provide insights for policy development and civil society's analysis and advocacy efforts.

Intermediaries should continue to benefit from safe-harbor protections for most of the user-generated and third-party content appearing on their platforms, so as not to encourage excessive restrictions that inhibit free expression. Laws should also protect "good Samaritan" rules allowing platforms to remove objectionable content in good faith, and reserve decisions on the legality of content for the judiciary. Independent, multistakeholder bodies and independent regulators with sufficient resources and expertise should be empowered to oversee the implementation of laws, conduct audits, and ensure compliance. Provisions within the EU's Digital Services Act—notably its transparency provisions, 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 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 circumvention technology and resist government orders to shut down internet connectivity or ban digital services. Service providers should use all available legal channels to challenge such requests from state agencies, whether they are official or informal, especially when they relate to the accounts of human rights defenders, civil society activists, journalists, or other at-risk individuals.

If companies cannot resist demands in full, they should ensure that any restrictions or disruptions are as limited as possible in duration, geographic scope, and type of content affected. Companies should 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 IN THE AGE OF AI

Even before the new wave of generative artificial intelligence (AI) products, AI was a key factor in the crisis of information integrity, serving as an intensifier in environments that were already vulnerable to manipulation. However, advancements in generative AI will supercharge the creation and dissemination of false and misleading content by state and nonstate actors, demanding a prompt response to safeguard access to reliable online information.

Governments

Governments should ensure that human rights principles, transparency, and independent oversight are embedded into AI regulation. Policymakers should specifically include robust protections against ineffective and unsafe systems, address algorithmic discrimination, require independent audits and human rights–based impact assessments, and mandate increased transparency regarding the design, testing, use, and effects of AI products. They should also require human review alternatives for AI decisions, such as in content moderation, and provide people with notice and clear explanations on how automated systems are being utilized. Governments should establish mechanisms for appeal and redress in cases of discrimination by AI systems. Finally, regulators should be empowered with sufficient resources and expertise to enforce their own rules and verify that companies are adhering to relevant laws.

Specifically, the US government should follow through on an executive order—in development at the time of writing—that includes protections outlined in the Office of Science and Technology Policy's Blueprint for an AI Bill of Rights, such as safeguards against algorithmic discrimination, limits on data use, and requirements for notice and explanation. In addition to such action, Congress should work with civil society and the executive branch to craft legislation that takes a rights-based approach to AI governance and transforms guiding principles into binding law. The US Federal Election Commission should also prohibit political parties, committees, and candidates from intentionally misrepresenting candidates in advertising that features AI-generated or manipulated imagery. In Europe, lawmakers negotiating on the proposed EU AI Act should, at minimum, ensure that the final text obligates companies to label AI-generated media and conduct fundamental rights impact assessments for uses of AI services that present risks for human rights.

Ultimately, strengthening information integrity is a long-term challenge that requires long-term solutions. A whole-of-society approach to fostering a diverse and reliable information space entails supporting independent online media and empowering ordinary people with the tools they need to identify false or misleading information. Civic education initiatives and digital literacy training can help people navigate complex media environments. Governments should also allocate funding to develop detection tools for AI-generated content, which will only become more important as these tools grow more sophisticated and more widely used. Finally, democracies should scale up efforts to support independent online media through financial assistance and innovative financing models, technical support, and professional development support.

Companies

The private sector has a responsibility to ensure their products contribute to, rather than undermine, a diverse and reliable information space. Companies should invest in staff working on issues related to public policy, integrity, trust and safety, and human rights, including regional and country specialists. These teams should collaborate closely with civil society groups around the world to understand the local impact of their products. Without such expertise, companies are ill-equipped to address the myriad of human rights violations and challenges to information integrity that can emerge online and have offline consequences.

Companies should develop effective methods to label AI-generated content, which entails using a cryptographic signature, and coordinate with civil society to standardize how the industry documents the provenance of specific content. Companies should also invest in developing software to detect AI-generated content.

Companies should ensure transparency and fairness in their policies and decisions, including by being open about how machine learning is used to train automated systems tasked with classifying, recommending, and prioritizing content for human review. They should also refrain from relying on automated systems to remove content without the opportunity for meaningful human review, and establish mechanisms for explanation, redress, and appeal. Finally, companies should work closely with independent researchers who can study the effects their services have on information integrity and free expression.

3. COMBAT DISPROPORTIONATE GOVERNMENT SURVEILLANCE

Governments worldwide have passed increasingly disproportionate surveillance laws, and can access a booming commercial market for surveillance tools, giving them the capacity to flout the rule of law and monitor the private communications of individuals inside and beyond their borders. The lack of data privacy safeguards in the United States and around the world exacerbates the harms of this 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. The US Congress should also close a legal loophole that allows US

government agencies to purchase personal data from data brokers rather than obtaining a warrant. And in the European Union (EU), policymakers negotiating over the final text of the proposed EU AI Act should ensure that it prohibits the use of AI in technologies that are widely known to infringe on human rights, including facial recognition, so-called "predictive policing," and real-time biometric identification.

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. In the United States, any reforms to Section 230 of the Communications Decency Act should not undermine the ability of intermediaries and service providers to offer robust encryption. Weakening encryption would endanger the lives of activists, journalists, members of marginalized communities, and ordinary people around the world.

The US government is leading the international community in its efforts to combat commercial spyware abuses. In March 2023, the administration of President Joseph Biden announced an executive order that, among other mandates, bars federal agencies from the "operational" use of commercial spyware products that pose a threat to national security or counterintelligence, or that could be employed by foreign governments to violate human rights or target people from the United States. While this is a welcome step forward, the White House should work with Congress to make the order's provisions permanent law through bipartisan legislation, ensuring that the prohibition remains in place under future administrations.

Governments should work closely with civil society to ensure that democracies' lists of prohibited companies are swiftly and appropriately updated as the industry evolves. The US Commerce Department's Bureau of Industry and Security has imposed special licensing requirements on several surveillance firms whose foreign government clients had used their technologies to target journalists, activists, and others. The addition of these firms to the bureau's Entity List was a positive development, and others engaged in such practices should be subjected to the same restrictions.

While the European Parliament launched a committee of inquiry to investigate the use of Pegasus and other spyware tools, the European Commission still needs to take formal action. The EU should follow the example of the United States and rein in the commercial surveillance market. Robust action from Brussels would send a very strong signal to spyware purveyors that their irresponsible trade will no longer be tolerated, particularly those operating within the EU's borders.

To guarantee effective international cooperation on spyware, the United States and like-minded democracies will need to encourage other governments to implement common standards. Governments that signed the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, as well as those that joined the Export Controls and Human Rights Initiative, should follow through on their commitments and encourage like-minded states to join.

Companies

Companies should mainstream end-to-end encryption in their products and uphold other robust security protocols, including by 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 publicly report 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.

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 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 the 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. Updated data-privacy protections should feature provisions that grant independent regulators and oversight mechanisms the ability, resources, and expertise to ensure compliance by foreign and domestic companies with 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 address these concerns through new regulations on commercial surveillance and data security. While an Advance Notice of Proposed Rulemaking was announced over a year ago, the process will not be completed for at least another year. In the meantime, Congress should ensure that the FTC has sufficient resources to develop and enforce meaningful regulations related to data protection.

In addition to the FTC's action, this year the Consumer Financial Protection Bureau (CFPB) announced proposed rulemaking under the Fair Credit Reporting Act, with the aim of holding the data broker industry accountable for the misuse of personal information. Among other principles, the CFPB should prioritize data minimization in its new regulations.

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. Democracies should live up to their own values at home in order to serve as more credible advocates for internet freedom abroad. Freedom House research shows that governments learn from one another, with leaders in less free countries often pointing to the problematic actions of democratic states to justify their repressive policies. Democratic governments everywhere have an opportunity to set a positive example by effectively tackling the genuine challenges of the digital age in a way that strengthens human rights and the global internet.

Governments

Governments should ensure that internet-related diplomacy is both coordinated among democracies and grounded in human rights. The effort should include identifying regional multilateral forums that are strategically placed to advance free and open internet principles. Democracies should facilitate dialogue among national policymakers and regulators, allowing them to share best practices and strengthen joint engagement at international standards-setting bodies.

Specifically, the Freedom Online Coalition (FOC) should improve its name recognition and its ability to drive diplomatic coordination and global action. It 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 mainstream its activity in other multilateral forums like the International Telecommunication Union and the Group of Seven. The FOC should create an internal mechanism by which member states' activities can be evaluated to ensure that they align with the coalition's principles. Finally, the FOC should diversify and expand its advisory network.

Governments should establish internet freedom programming as a vital component of their democracy assistance, incorporating funding for digital security and cyber 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. Policymakers should advance efforts to strengthen regulatory and judicial independence, enhance technical literacy among judges and others within the legal and regulatory system, and provide other financial and administrative resources for strategic litigation.

Democracies should collectively impose meaningful penalties, including targeted sanctions, on anyone directing or engaging in reprisals against individuals exercising free expression online. 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 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. It should be standard practice to raise the names of those detained for their online content, to request information or specific action related to their treatment, and to call for their release and the repeal of laws that improperly criminalize online expression.

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, companies should coordinate with democratic governments to confirm that they are not engaging in excessive risk-mitigation activities that might negatively and needlessly affect civilians who have not themselves been sanctioned.

Methodology

WHAT WE MEASURE

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

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

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

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

THE RESEARCH AND SCORING PROCESS

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

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

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

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

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

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

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

Checklist of Questions

A. OBSTACLES TO ACCESS

(*0–25 POINTS*)

1. **Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?** (*0–6 points*)
   - Do individuals have access to high-speed internet services at their home, place of work, 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 seen to be fair and to take meaningful notice of comments from stakeholders in society?
   - Are decisions taken by regulatory bodies seen to be apolitical and independent from changes in government?
   - Are decisions taken by regulatory bodies seen to be protecting internet freedom, including by ensuring service providers, digital platforms, and other content hosts behave fairly?

B. LIMITS ON CONTENT

(*0–35 POINTS*)

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

2. **Do state or nonstate actors employ legal, administrative, or other means to force publishers, digital platforms, or other content hosts 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, and 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, 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, 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 self-regulatory mechanisms and oversight bodies 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 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 place legal or other restrictions (e.g. criminal provisions, detentions, surveillance) for the purpose of restricting free assembly and association online?

C. VIOLATIONS OF USER RIGHTS

(*0–40 POINTS*)

1. **Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?** (*0–6 points*)
   - Does the constitution contain language that provides for freedom of expression, access to information, and press freedom generally?
   - Are there laws or binding legal decisions that specifically protect online modes of expression and access to information?
   - Do executive, legislative, and other governmental authorities comply with these legal decisions, and are these decisions effectively enforced?
   - Are online journalists and commentators accorded strong rights and protections to perform their work?

- 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 residents (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, 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?

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?
   - 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 85 researchers, who come from civil society organizations, academia, journalism, and other backgrounds, covering 70 countries. In repressive environments, Freedom House takes care to ensure researchers' anonymity and/or works with experts living abroad.

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

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

CONTRIBUTORS

Freedom House staff

- **Adrian Shahbaz**, Vice President of Research and Analysis
- **Allie Funk**, Research Director for Technology and Democracy
- **Jennifer Brody**, Deputy Director of Policy and Advocacy for Technology and Democracy
- **Kian Vesteinsson**, Senior Research Analyst for Technology and Democracy
- **Grant Baker**, Research Analyst for Technology and Democracy
- **Cathryn Grothe**, Research Analyst for Middle East and North Africa
- **Matthew Barak**, Research Associate
- **Maddie Masinsin**, Community Engagement Specialist for Technology and Democracy
- **Rucha Modi**, former Research Associate 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*. Michael Abramowitz, Gerardo Berthin, Nicole Bibbins Sedaca, Annie Boyajian, Sarah Cook, Yana Gorokhovskaia, Nate Schenkkan, and Lara Shane provided valuable feedback on the summary of findings. Gabriela Ivanova, Tsering Lhamo, Dasha M., Eva Stanley, and Jessica White provided research assistance. Danielle Dougall and Alex Rochefort served as research consultants.

Report authors

- **Angola:** Africa Monitor Intelligence
- **Argentina:** Eduardo Ferreyra, independent researcher
- **Armenia:** Samvel Martirosyan, Co-Founder of CyberHUB-AM
- **Australia:** Samantha Floreani and Lizzie O'Shea, Digital Rights Watch
- **Azerbaijan:** Arzu Geybulla, 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
- **Cambodia:** Sopheap Chak, Cambodian Center for Human Rights
- **Canada:** Allen Mendelsohn, McGill University
- **Colombia:** Susana Echaverría Medina, El Veinte
- **Costa Rica:** Óscar Mario Jiménez Alvarado, Fernando José Martínez de Lemos, Johanna Rodríguez López, Programa de Libertad de Expresión, Programa de Libertad de Expresión y Derecho a la Información (PROLEDI), Universidad de Costa Rica (UCR)
- **Cuba:** Ted A. Henken, Baruch College, City University of New York
- **Ecuador:** Ana Aguilera A., Susana Cadena V., Emily Fonseca J., Julio López P., Diego Pérez V., Carolina Torres G., and Margarita Yépez V., Fundación Datalat
- **Estonia:** Hille Hinsberg and Florian Marcus, Proud Engineers
- **Ethiopia:** Atnafu Brhane, Center for Advancement of Rights and Democracy (CARD)
- **France:** Théophile Lenoir, University of Milan
- **Georgia:** Teona Turashvili, Institute for Development of Freedom of Information (IDFI)
- **Germany:** Matthieu Binder and Paul Ritzka, iRights.Lab
- **Hungary:** Dalma Dojcsák, Hungarian Civil Liberties Union

- **Iceland:** Arnaldur Sigurðarson, independent researcher
- **Indonesia:** Southeast Asia Freedom of Expression Network (SAFEnet)
- **Iran:** Mahsa Alimardani, University of Oxford, Oxford Internet Institute
- **Iraq:** Hayder Hamzoz and Assia Abdulkareem, INSM Foundation for Digital Rights
- **Italy:** Philip Di Salvo, postdoctoral researcher, School of Humanities and Social Sciences, Universität St. Gallen and Antonella Napolitano, independent researcher
- **Japan:** Hamada Tadahisa, Japan Computer Access for Empowerment
- **Lebanon:** Marianne Rahme, SMEX
- **Libya:** Jabir Zain, Libyan Center for Freedom of the Press
- **Malawi:** Jimmy Kainja, University of Malawi
- **Malaysia:** Kelly Koh, Sinar Project
- **Mexico:** Vladimir Cortés, independent researcher
- **Myanmar:** Free Expression Myanmar
- **Nicaragua:** IPANDETEC
- **Nigeria:** Adeboro Odunlami, independent researcher
- **Philippines:** Vino Lucero, independent researcher
- **Serbia:** Mila Bajić, Asja Lazarević, Bojan Perkov, SHARE Foundation
- **Singapore:** Kirsten Han, independent researcher
- **South Africa:** Tshepiso Hadebe, PPM Attorneys
- **South Korea:** Yenn Lee, SOAS University of London
- **Sudan:** Digital Rights Lab - Sudan
- **Taiwan:** Ming-Syuan Ho, independent researcher
- **Thailand:** Emilie Pradichit and Letitia Visan, Manushya Foundation
- **The Gambia:** Nasiru Deen, independent researcher
- **Tunisia:** Yosr Jouini, independent researcher
- **Turkey:** Gürkan Özturan, Media Freedom Rapid Response Coordinator at the European Centre for Press and Media Freedom
- **Ukraine:** Olga Kyryliuk, independent researcher
- **United Kingdom:** Dr. Edina Harbinja, Aston University
- **United States:** Rachel Lau, independent researcher
- **Uzbekistan:** Ernest Zhanaev, doctoral researcher, University of St Andrews
- **Venezuela:** Raisa Urribarri, Universidad de Los Andes
- **Vietnam:** Trinh Huu Long, Legal Initiatives for Vietnam
- **Zambia:** Bulanda T. Nkhowani, independent researcher
- **Zimbabwe:** Nompilo Simanje, Africa Advocacy and Partnerships Lead, International Press Institute

Researchers for Bahrain, Bangladesh, Belarus, China, Egypt, Ghana, India, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Morocco, Pakistan, Russia, Rwanda, Saudi Arabia, Sri Lanka, Uganda, and the United Arab Emirates wished to remain anonymous.

Advisers

- **Elwaleed Ahmed**, independent researcher
- **Eto Buziashvili**, Atlantic Council's Digital Forensic Research Lab
- **Alejandra Caraballo**, Harvard Law School Cyberlaw Clinic
- **Hakeem Dawd Qaradaghi**, independent researcher
- **Renee DiResta**, Technical Research Manager, Stanford Internet Observatory
- **Piseth Duch**, human rights lawyer
- **Katie Harbath**, Founder and CEO, Anchor Change
- **Daphne Keller**, Director of the Program on Platform Regulation at Stanford Cyber Policy Center
- **Jumana Musa**, National Association of Criminal Defense Lawyers
- **Peace Oliver Amuge**, Africa Regional Strategy Lead at The Association for Progressive Communications
- **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

For this report's main essay, Freedom House identified several ways in which AI exacerbated digital repression during the coverage period and collected the relevant information across 70 countries covered by *Freedom on the Net*. The essay's analysis and data points were partly informed by the individual *Freedom on the Net* country reports, written by external report authors that are listed above. Freedom House staff also conducted additional research and drew on the important work of various media groups, civil society organizations, and other experts, including but not limited to the Artificial Intelligence Incident Database, the Center for Democracy and Technology, the Center for European Policy Analysis, Cloudflare, Graphika, NewsGuard, the Open Observatory of Network Interference (OONI), and the OECD AI Policy Observatory. Research and analysis from experts including Robert Chesney, Danielle Citron, Alex C. Engler, Steven Feldstein, Matt Fredrikson, J. Zico Kolter, Odanga Madung, Brian Obilo, Grigore Pop-Eleches, Margaret E. Roberts, Zifan Wang, Lucan A. Way, Samuel C. Woolley, Eddie Yang, and Andy Zou also influenced the essay. Freedom House furthermore wishes to acknowledge the academics, researchers, and civil society activists who have worked to document, respond to, and mitigate AI-driven harms, including those not addressed in this report.

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

Shahbaz, Funk, Brody, Vesteinsson, Baker, Grothe, Barak, Masinsin, Modi, Sutterlin eds. *Freedom on the Net 2023*, Freedom House, 2023, freedomonthenet.org.

Shahbaz, Funk, and Vesteinsson, "The Repressive Power of Artificial Intelligence," in Shahbaz, Funk, Vesteinsson, Brody, Baker, Grothe, Barak, Masinsin, Modi, Sutterlin eds. *Freedom on the Net 2023*, Freedom House, 2023, freedomonthenet.org.

"Angola," in Shahbaz, Funk, Brody, Vesteinsson, Baker, Grothe, Barak, Masinsin, Modi, Sutterlin eds. Freedom on the Net 2023, *Freedom House, 2023*, freedomonthenet.org.

Board of Trustees

* Denotes members of the Executive Board

President
Michael J. Abramowitz

Chair
The Hon. Jane Harman*

Vice Chair
Goli Ameri*
Peter Bass*

Treasurer
Robert Keane*

Secretary
Cater Lee*

Trustees
Carol C. Adelman*
Sewell Chan
Michael Chertoff*
Carole Corcoran
Rodger Desai
Martin Etchevers
Mathea Falco
David L. Fogel
Francis Fukuyama
Jonathan Ginns
Mark Goodman*
Dionisio Gutierrez
Nina Jacobson
Thomas Kahn
Rachel Kleinfeld*
Howard Konar
Faith Morningstar
Dr. Sharon S. Nazarian
Lynn Novick
Sushma Palmer
Vivek Paul
Maurice A. Perkins
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.

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

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