Freedom on the Net 2022

Countering an Authoritarian Overhaul of the Internet

At home and on the international stage, authoritarians are on a campaign to divide the open internet into a patchwork of repressive enclaves.

WRITTEN BY
Adrian Shahbaz
Allie Funk
Kian Vesteinsson

Key Findings

Global internet freedom declined for the 12th consecutive year. The sharpest downgrades were documented in Russia, Myanmar, Sudan, and Libya. Following the Russian military's illegal and unprovoked invasion of Ukraine, the Kremlin dramatically intensified its ongoing efforts to suppress domestic dissent and accelerated the closure or exile of the country's remaining independent media outlets. In at least 53 countries, users faced legal repercussions for expressing themselves online, often leading to draconian prison terms.

Governments are breaking apart the global internet to create more controllable online spaces. A record number of national governments blocked websites with nonviolent political, social, or religious content, undermining the rights to free expression and access to information. A majority of these blocks targeted sources located outside of the country. New national laws posed an additional threat to the free flow of information by centralizing technical infrastructure and applying flawed regulations to social media platforms and user data.

China was the world's worst environment for internet freedom for the eighth consecutive year. Censorship intensified during the 2022 Beijing Olympics and after tennis star Peng Shuai accused a high-ranking Chinese Communist Party (CCP) official of sexual assault. The government continued to tighten its control over the country's booming technology sector, including through new rules that require platforms to use their algorithmic systems to promote CCP ideology.

A record 26 countries experienced internet freedom improvements. Despite the overall global decline, civil society organizations in many countries have driven collaborative efforts to improve legislation, develop media resilience, and ensure accountability among technology companies. Successful collective actions against internet shutdowns offered a model for further progress on other problems like commercial spyware.

Internet freedom in the United States improved marginally for the first time in six years. There were fewer reported cases of targeted surveillance and online harassment during protests compared with the previous year, and the country now ranks ninth globally, tied with Australia and France. The United States still lacks a comprehensive federal privacy law, and policymakers made little progress on the passage of other legislation related to internet freedom. Ahead of the

November 2022 midterm elections, the online environment was riddled with political disinformation, conspiracy theories, and online harassment aimed at election workers and officials.

Human rights hang in the balance amid a competition to control the web. Authoritarian states are vying to propagate their model of digital control around the world. In response, a coalition of democratic governments has increased the promotion of online human rights at multilateral forums, outlining a positive vision for the internet. However, their progress remains hampered by problematic internet freedom practices in their own countries.

Introduction

At home and on the international stage, authoritarians are on a campaign to divide the open internet into a patchwork of repressive enclaves. More governments than ever are exerting control over what people can access and share online by blocking foreign websites, hoarding personal data, and centralizing their countries' technical infrastructure. As a result of these trends, global internet freedom has declined for a 12th consecutive year.

Rising digital repression in many countries mirrored broader crackdowns on human rights over the past year. Nowhere was this clearer than in Russia, Myanmar, Libya, and Sudan, which experienced the world's steepest declines in internet freedom. Online censorship reached an all-time high, with a record number of governments blocking political, social, or religious content, often targeting information sources based outside of their borders. More than three-quarters of the world's internet users now live in countries where authorities punish people for exercising their right to free expression online.

Alarmingly, these antidemocratic abuses are not the only factor behind the splintering of the internet into national segments. Some governments are clearly cultivating a domestic digital space where state-endorsed narratives dominate and independent media, civil society, and already marginalized voices are more easily suppressed. But others are inadvertently contributing to country-based barriers through their efforts to tackle disinformation, protect user data, and deter genuine cybercrimes. Whatever the intention, however, the growing fragmentation of the internet comes with serious consequences for fundamental rights including freedom of expression, access to information, and privacy, particularly for people living under authoritarian regimes or in backsliding democracies.

Explore the Report

Tracking the Global Decline

The Shattering of the Global Internet

A Resilient Internet for a More Democratic Future

A more fragmented internet

The internet has always been subject to some degree of fracturing along national borders, but increased state intervention in the last year has dramatically accelerated the process. This report identifies three main causes of fragmentation, all of which contributed to declining respect for human rights online: restrictions on the flow of news and information, centralized state control over internet infrastructure, and barriers to cross-border transfers of user data.

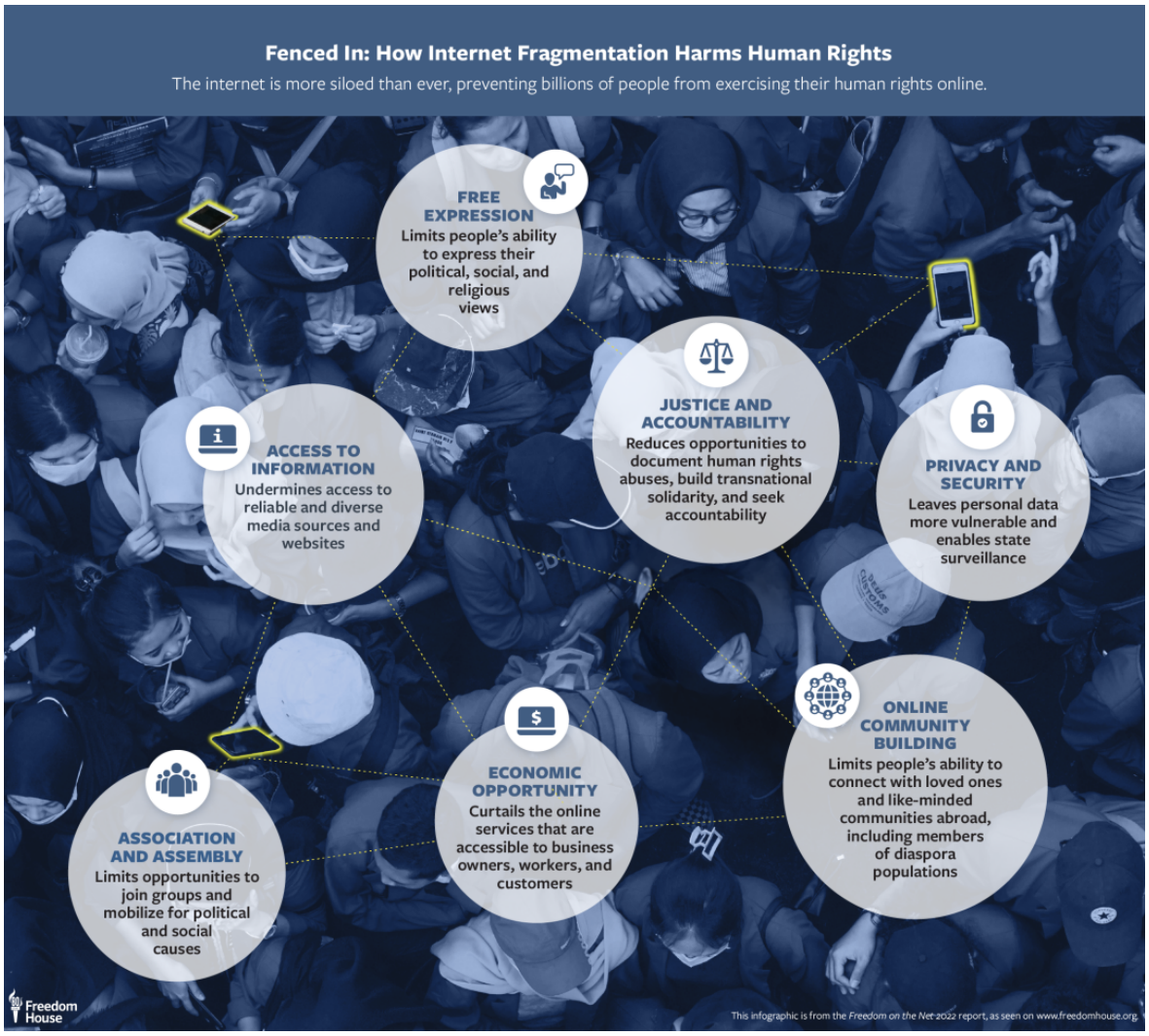
While the physical network of the global internet remains intact, a growing number of users only have access to an online space that mirrors the views of their government and its interests. Authorities in 47 of the 70 countries covered by *Freedom on the Net* have limited users' access to information sources located outside of their borders. Virtually all of these restrictions constitute

clear infringements of the Universal Declaration of Human Rights, which codifies the right "to seek, receive, and impart information and ideas through any media and regardless of frontiers." In most cases, entrenched and aspiring authoritarian leaders sought to contain online dissent by preventing residents from reaching information sources based in countries with a greater level of media freedom.

Entrenched and aspiring authoritarian leaders sought to contain online dissent by preventing residents from reaching global information sources.

This increasing fragmentation is part of a global, multifaceted competition for control over the digital sphere. For most of the period since the internet's inception, representatives of the private sector, civil society, and the technical community have participated in a consensus-driven process to harmonize security standards and technical protocols. This has resulted in a decentralized infrastructure that speaks a common language, enabling users to communicate with one another and access information regardless of location. Authoritarian powers have long sought to displace this multistakeholder model of internet governance with one that promotes cyber sovereignty, or greater control by states. Diplomats from China and Russia have made inroads at institutions like the International Telecommunication Union (ITU), seeking to transform the United Nations agency into a global internet regulator that advances authoritarian interests. Doing so would fundamentally alter the open internet, preventing billions of people from communicating with one another and accessing life-changing resources without explicit permission from their governments.

A cohort of democracies are pushing back. Having previously focused on a narrower set of economic and security interests linked to countering Beijing, the United States has more recently shown promising signs of reengagement in cyber diplomacy with the aim of promoting a positive vision of democracy in the digital age. The European Union (EU) has also moved forward with innovative and rights-respecting regulatory approaches to address harms that have been exacerbated by the internet. But many democracies have yet to significantly improve respect for online rights within their own borders. Of the 35 countries covered by this report that participated in the US-hosted Summit for Democracy, 13 experienced an internet freedom decline over the past year, as did 10 of the 18 *Freedom on the Net* countries that signed the US-led Declaration for the Future of the Internet. By adopting flawed policies at home, democracies risk undermining the very values they seek to defend abroad, while potentially cutting off residents of authoritarian countries from a freer and more open internet.



Protecting human rights online through democratic resilience

The technologies associated with the global internet have fostered connections and common interests among different people and communities, facilitated more transparent and participatory governance, and brought tremendous direct and indirect economic benefits. However, the rapid digitization of media and communication has also generated new opportunities for manipulation, extremism, and repression. Policymakers have been too slow in addressing the hazards that accompany technological change, and their emphasis on state-level digital threats—grouped under terms such as information war, cyberwar, and trade war—has often elevated national security and economic considerations over the fundamental rights of individuals. The reality is that economic and security interests are directly linked to respect for individual rights.

Lasting solutions to disinformation, online harassment, and other harms presented by digital tools are unlikely to be achieved through a fragmentation of the internet. Simply imposing strict national laws onto a global information system is bound to be ineffective. Beijing's efforts to build and maintain a Great Firewall, for example, have done little to address societal concerns about privacy, cybersecurity, corporate malfeasance, false content, and abusive online behavior. It may be difficult to prevent Beijing, Moscow, and Tehran from persisting in their efforts to isolate their populations, but there remains an opportunity to convince many less repressive states that an open internet is in their best interest.

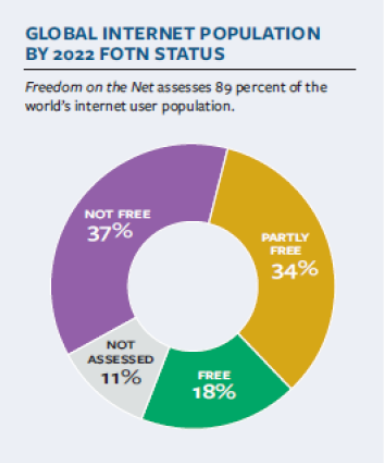
Greater focus should be placed on developing political and societal resilience in the face of these harms. Already, journalists, human rights defenders, and advocacy organizations have been at the forefront of many recent successes that strengthened democratic resilience in the digital sphere. Broad coalitions have bolstered international norms against internet shutdowns, which occurred in fewer countries over the past year. Collaborative investigations into the purveyors of surveillance software have resulted in growing awareness of an underregulated industry that continues to target state officials, journalists, activists, and members of diaspora communities. Whistleblowers have

done the public a great service by exposing the inadequacies and failures of influential technology companies.

Democratic leaders should recommit to preserving the benefits of a free and open internet. True resilience requires new regulations that enshrine protections for human rights in the digital age, stronger multilateral coordination on cybercrime and corporate accountability, and deeper investment in civil society, which so often drives collective action to defend internet freedom and resist digital authoritarianism.

Tracking the Global Decline

A rundown of prominent changes to countries' internet freedom scores



Global internet freedom has declined for the 12th consecutive year. The environment for human rights online deteriorated in 28 countries, though 26 countries registered net gains—the largest number of improvements since the inception of the project. The sharpest decline occurred in Russia, followed by Myanmar, Sudan, and Libya, while The Gambia and Zimbabwe experienced major improvements. The United States ranked ninth overall, and Iceland was once again the top performer. For the eighth consecutive year, China was found to have the worst conditions for internet freedom.

Freedom on the Net is an annual study of human rights in the digital sphere. The project assesses internet freedom in 70 countries, accounting for 89 percent of the world's internet users. This report, the 12th in its series, covered developments between June 2021 and May 2022. More than 80 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, as well as policy recommendations for governments and tech companies.

The Kremlin's invasion of Ukraine puts internet freedom under threat

Internet freedom in Russia declined by seven points in the period surrounding the government's brutal invasion of Ukraine in February 2022, reaching an all-time low and representing this year's largest national decline in *Freedom on the Net*. Within weeks of the invasion, the Kremlin blocked Facebook, Instagram, and Twitter, depriving Russians of access to reliable information about the war and limiting their ability to connect with users in other countries. The government also blocked more than 5,000 websites, compelled media outlets to refer to the invasion as a "special military operation," and introduced a law prescribing up to 15 years in prison for those who spread "false information" about the conflict. The regime's increasing restrictions, both before and after the invasion was launched, significantly raised the risks associated with online activism and hastened the closure or exile of the country's remaining independent media outlets.

Internet freedom in Russia reached an all-time low following the government's brutal invasion of Ukraine.

The Russian military's actions in Ukraine also undermined that country's internet freedom. In the southern city of Kherson, Russian troops forced service providers to reroute internet traffic through Russian networks during the spring and summer of 2022, leaving Ukrainian users without access to major social media platforms and a plethora of Ukrainian and international news sites. Though

online media outlets have bravely continued to cover the invasion, their reporters faced great danger while carrying out their work. Several journalists affiliated with such websites were killed by Russian forces.

The Ukrainian government and people have shown astonishing resilience during the invasion. Government officials and telecommunications companies worked together to repair internet infrastructure and ensure access to online resources and information, which can be life-saving in the midst of an armed conflict. Some 11,000 Starlink stations were deployed to provide satellite-based internet service as part of a collaboration involving the government, the US technology firm SpaceX, and other partners. Ukrainian telecom operators also enabled users to switch between carriers when their primary carrier's signal was unavailable, and they undertook major efforts to deliver Wi-Fi access to bomb shelters. Immediately after Russian forces invaded the country, the Ukrainian company Ajax Systems collaborated with the government to launch a mobile application—downloaded more than four million times as of March—that alerts users about incoming air raids.

Coups and elections drive major declines and improvements

Internet freedom declined by five points in Myanmar, contributing to a precipitous 19-point decline over the past two years. The country now hosts the second worst environment for human rights online, outperforming only China. Since the military junta seized power from an elected civilian government in February 2021, it has cemented its censorship regime, blocking all but 1,200 websites, restricting access to major social media platforms, and imposing local internet shutdowns. The few online resources that remained accessible during the year were dominated by promilitary voices, and activists, journalists, and ordinary users continued to be forcibly disappeared, detained, and tortured. The junta compelled the Norwegian service provider Telenor to sell its operations in the country to a military-aligned company, fully consolidating its control over the telecommunications sector.

Sudan's score fell by four points after military leaders staged a coup and dissolved the country's transitional government in October 2021, marking a devastating setback for Sudanese democracy. The military voided articles of the interim constitution that protected fundamental rights and declared a state of emergency that lasted until May 2022. As Sudanese civilians mobilized mass protests in response, authorities restricted internet connectivity, blocked social media platforms, and assaulted and arrested journalists.

Internet freedom in Nicaragua dropped by three points amid an election in November 2021 that featured a harsh clampdown on opposition leaders, dissidents, and independent journalists. Repressive legislation such as the Cybercrime Law paved the way for increased self-censorship and lengthy prison sentences against critical users.

In Hungary, the status of internet freedom declined from Free to Partly Free, mirroring the country's broader democratic decline under the leadership of Prime Minister Viktor Orbán. During opposition primary elections in September and October 2021, in which voters chose candidates to challenge Orbán and his ruling party, cyberattacks from unknown sources plagued electronic voting systems and independent news outlets in the country. Election organizers were forced to suspend voting after their computer system suffered an attack, and independent news sites were taken offline before the announcement of electoral results. Months earlier in July, an investigation revealed that at least three journalists had been targeted with Pegasus, an infamous spyware tool developed by the Israeli firm NSO Group.

In The Gambia, internet freedom improved by three points, contributing to a 23-point improvement since the end of former president Yahya Jammeh's repressive regime in 2017. Gambians mobilized online without restriction during the December 2021 presidential election, in which incumbent Adama Barrow secured a second term. The Barrow administration also passed a landmark law guaranteeing the right to public information, an important step for transparency and accountability.

New and persistent threats to free expression worldwide

Freedom on the Net found that officials in at least 53 countries charged, arrested, or imprisoned internet users in retaliation for posts about political or social causes. In Libya, which suffered this year's third-largest score decline alongside Sudan, users who shared criminal commentary or reporting online have been forcibly disappeared before reemerging in detention. Rwandan authorities sentenced a YouTube commentator whose videos criticized the government to 15 years in prison in September 2021.

Authorities in at least 40 countries blocked social, political, or religious content online, an all-time high in *Freedom on the Net*. Internet users in Jordan reported that the website of the International Consortium of Investigative Journalists was briefly blocked in October 2021, after the organization published leaked financial documents that exposed the secret wealth of the country's king and other world leaders. In Belarus, authorities blocked the websites of civil society organizations throughout

the coverage period, part of a wholescale assault on the groups that included raids, arrests, and forced closures.

In at least 22 countries, government officials blocked access to social media or communications platforms. Some blocks were imposed to coerce the companies into compliance with requirements that they open in-country offices, store data within the country, or otherwise change their operations in ways that facilitate enforcement of government censorship or data requests. In Uzbekistan, authorities blocked a range of international social media and messaging apps in July and November 2021 on the grounds that they failed to comply with localization requirements in a data protection law; access to most platforms was restored by August 2022. In March 2022, a judge on Brazil's Supreme Court reversed an order that would have banned Telegram, after the app agreed to remove content that was flagged as disinformation and announced that it would appoint a local representative. Nigerian officials rescinded a seven-month block on Twitter in January 2022, claiming that the company had agreed to establish a physical presence in the country.

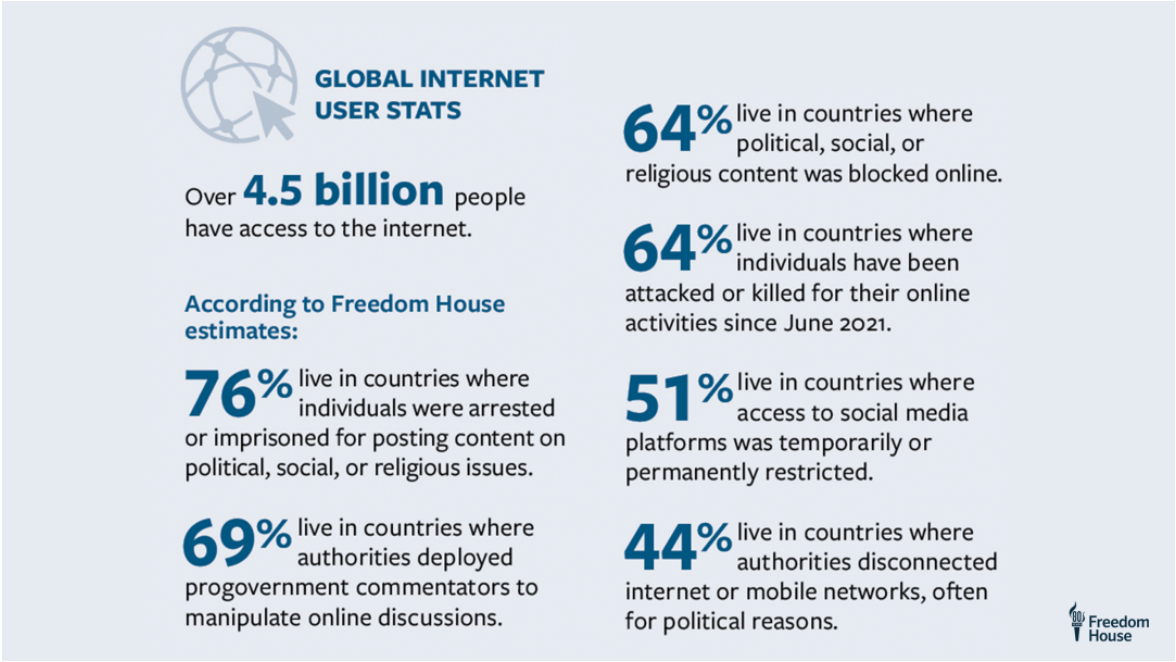
The future of internet freedom in "swing states"

Countries including Brazil and Nigeria are often referred to as swing states due to their potential regional or global influence over the future of internet governance. They have oscillated between protecting and undermining human rights online, with many ranked Partly Free by *Freedom on the Net*. Progress in these countries could ensure the survival of a free and open internet, or they could join authoritarian powers in promoting the more closed model of cyber sovereignty. Democratic institutions in some swing states intervened to protect human rights online during the coverage period. The Indian Supreme Court ordered the government to reevaluate the country's colonial-era sedition law, which has increasingly been used to charge online dissidents, in May 2022—even as political leaders sought to extend control over online content through problematic new legislation. Brazilian lawmakers enshrined the protection of personal data in the constitution in February 2022, a landmark action that elevated privacy rights above the whims of any government or simple legislative majority.

Progress in "swing states" could ensure the survival of a free and open internet.

But the decision came amid a contentious election year, in which President Jair Bolsonaro and his allies have bombarded the online space with false claims about electoral fraud. In October 2021, Kenya's highest court paused the implementation of an expansive biometric identity-card system until it could meet appropriate standards for data protection. President Guillermo Lasso of Ecuador vetoed provisions of a law that criminalized the disclosure of secrets online in June 2021, protecting digital media outlets from a serious legal threat.

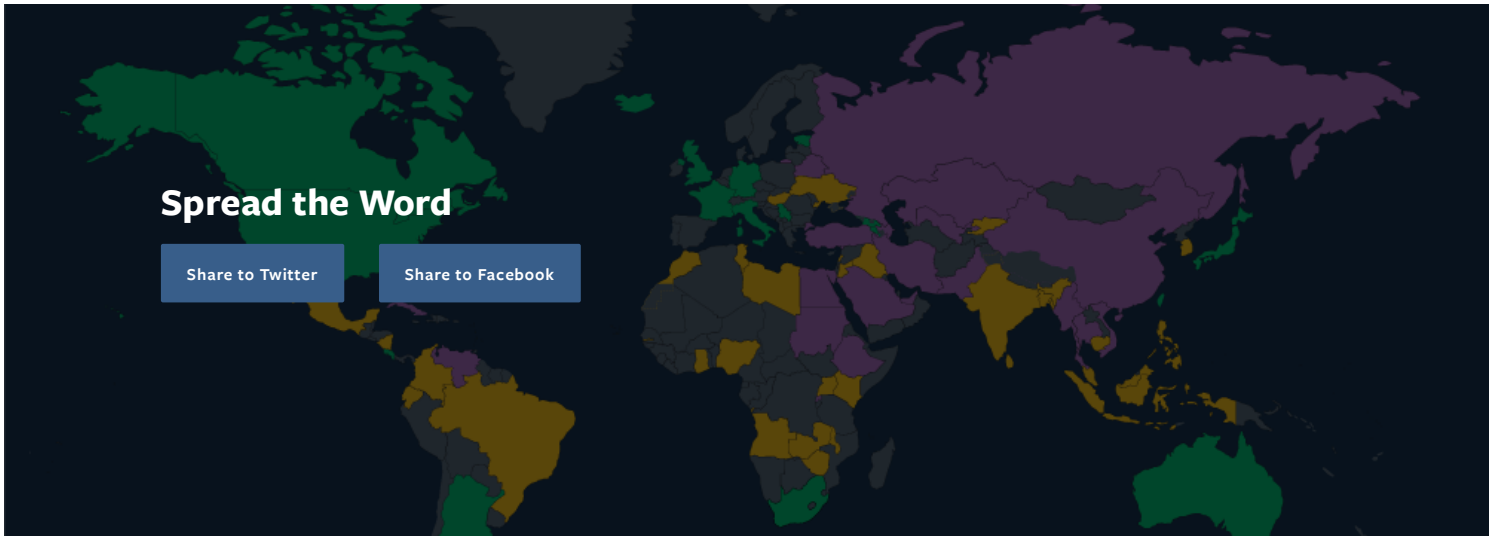
Other countries in this group pursued practices that increased digital repression and undermined the diversity of the information space. In Tunisia, President Kaïs Saïed suspended parts of the constitution, imposed overly broad rules barring what the state deems to be "false" information, and oversaw the arrest of his online critics—an alarming turn for the country with the Arab world's highest internet freedom score. Indonesian authorities briefly blocked several websites after the coverage period, including Yahoo and PayPal, to force compliance with a repressive law that requires companies to register with the government, appoint a local liaison, and remove content under tighter timelines.



The world's most repressive online environment

For the eighth consecutive year, China remained the world's worst environment for internet freedom. Content related to the 2022 Beijing Olympics and the COVID-19 pandemic remained heavily censored during the coverage period, particularly as Shanghai residents shared their experiences amid a disastrous two-month lockdown that began in April 2022. The government also intensified censorship of online content related to women's rights and suppressed social media campaigns against sexual assault and harassment, including through the detention of tennis star Peng Shuai after she alleged on the social media platform Weibo that she was sexually assaulted by senior CCP official Zhang Gaoli. Separately, journalists, human rights activists, members of religious and ethnic minority groups, and ordinary users were detained for sharing online content, with some facing harsh prison sentences.

Government officials instituted new policies to tighten their control over Chinese technology companies. The main internet regulator issued guidance requiring platforms to align their content moderation and recommendation systems with "Xi Jinping Thought"—the official ideology of the current CCP leader. Another set of draft rules would impose heavy penalties on companies that enable Chinese internet users to bypass the Great Firewall. Meanwhile, the country's data protection framework, which took effect in November 2021, established baseline safeguards for personal data held by Chinese companies—though it failed to apply the same standards to data held or requested by the government.



For the United States, progress abroad and stalemate at home

The administration of US president Joseph Biden made the promotion of internet freedom a top priority of its foreign policy. In April 2022, the White House helped bring together more than 60 governments to sign the Declaration for the Future of the Internet, a nonbinding agreement to advance a positive vision of the internet. The US State Department established its Bureau of Cyberspace and Digital Policy, helped launch the Export Controls and Human Rights Initiative, and revealed that it would chair the Freedom Online Coalition in 2023. Similarly, the US Agency for International Development announced an investment of up to $20 million annually to dramatically expand its digital democracy work. This flurry of activity on the global stage stood in stark contrast to the lack of movement at home. While internet freedom improved for the first time in six years, the change was marginal, and proposed laws that would strengthen human rights online and increase tech-related transparency made little progress. The continued lack of a comprehensive federal privacy law and incomplete reforms to surveillance rules have allowed government agencies to simply purchase Americans' data from shadowy brokers with little oversight or safeguards.

The lack of a comprehensive privacy law and incomplete reforms to surveillance rules have allowed government agencies to simply purchase Americans' data from shadowy brokers.

The Supreme Court decision that overturned *Roe v. Wade* and denied a constitutional right to abortion also prompted renewed concerns about law enforcement access to location information, browsing histories, and other forms of data that could be used for criminal and civil investigations in US jurisdictions where legal access to reproductive health care is restricted.

During the coverage period, mass denial of the outcome of the 2020 presidential election by former president Donald Trump and his supporters, driven in part by online conspiracy theories and disinformation, polluted the information environment and seeped into the broader American political system. Election deniers have leveraged online support to mount viable candidacies for public office ahead of the November 2022 midterm balloting. Disinformation about stolen elections and supposed vulnerability to fraud has fueled calls for citizens to "protect" the vote by force if necessary. Election workers and administrators have reported receiving a barrage of online threats and harassment, leading large numbers of them to resign out of fear for their own safety. In effect, such disinformation and intimidation have undermined the basic security of US electoral mechanisms, provided Republican Party leaders in many states with a false justification for new antifraud measures that could restrict access to voting or distort the counting and certification processes, and set the stage for future unrest by eroding public trust in any unfavorable results.

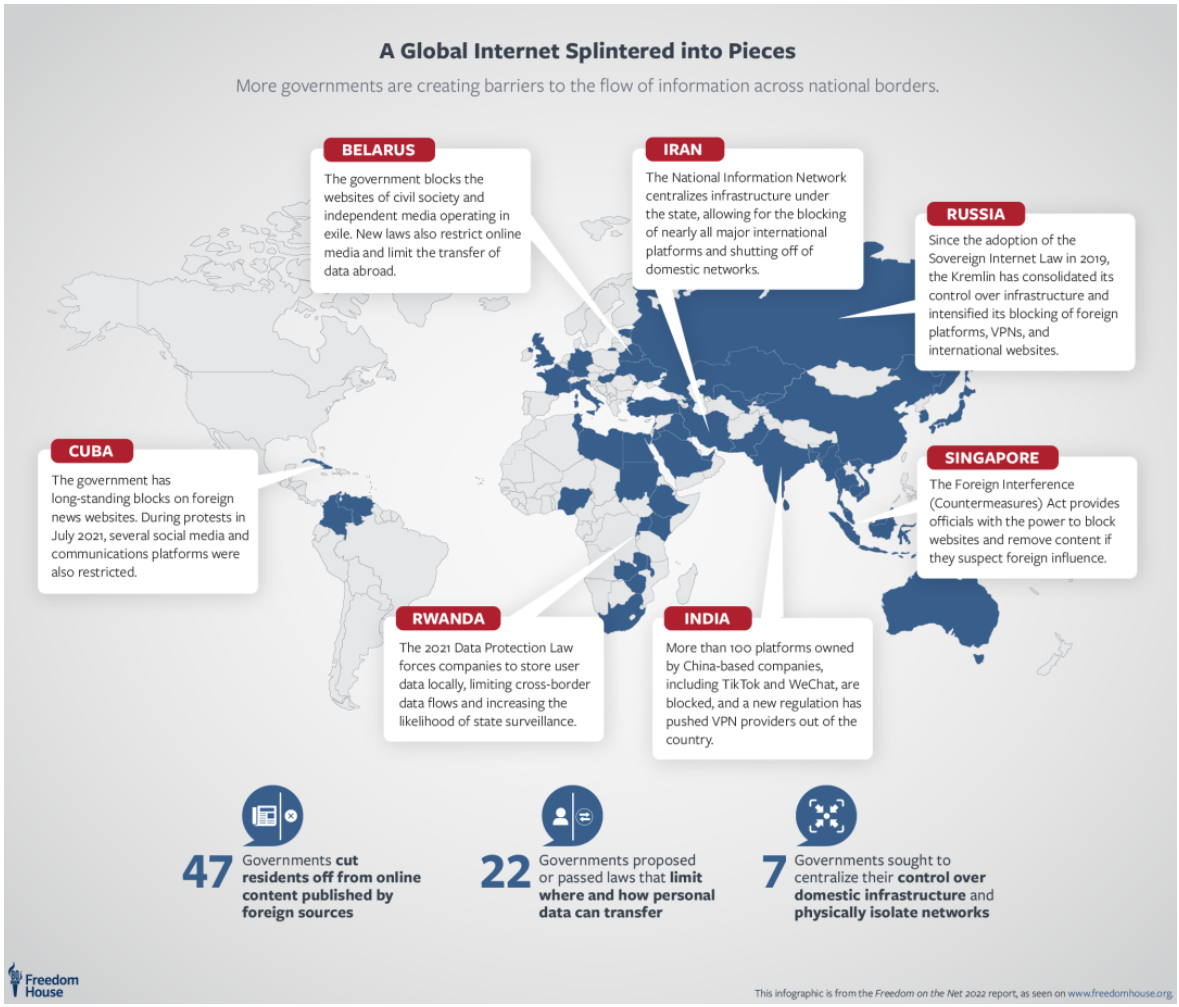
The Shattering of the Global Internet

The internet is more fragmented than ever, preventing billions of people from exercising their human rights online. Authorities in over two-thirds of the countries surveyed in this report have used their legal and regulatory powers to limit access to foreign information sources, leaving residents in a domestic information space that is effectively shaped by the state. More governments are also passing legislation that places guardrails around the flow of user data across borders, with mixed consequences for the global internet and human rights. The most perilous laws purport to protect privacy even as they delegate oversight to regulators beholden to the political leadership or force data to be stored in less secure settings.

Few if any countries have taken the extreme step of disconnecting entirely from the global internet on a technical level. But a small number of authoritarian leaders are following the CCP in reengineering their domestic networks to allow greater control over technical infrastructure. Their success remains constrained by the daunting economic and societal costs of such measures, as well as the endurance of international norms supporting an open global internet.

The myriad of national regulations and practices that contribute to fragmentation—intentionally or not—are being imposed by governments across the democratic spectrum, but there are crucial distinctions. Authoritarian regimes in countries such as China, Iran, and Russia are seeking to wall their people off from the rest of the world. More democratic measures typically seek to enforce

rights-protecting legislation that addresses abusive company behavior or genuine online harms. Though accomplished through state intervention, these policies are often paired with safeguards that allow for the continued flow of information and services across borders, so long as partners ensure a similar level of protection for users' rights.



Isolating users from outside information

In response to both real and purported threats online, authorities in at least 47 countries cut residents off from the flow of news and information across borders. Some governments alleged foreign meddling to justify new censorial regulations, while others imposed localized shutdowns of internet service, plunging users into digital darkness in a bid to suppress information about human rights abuses. In tandem with this censorship, many political leaders bolstered support for state-aligned social media platforms that are more receptive to their demands.

The restrictions were largely imposed in countries that are designated as Not Free or Partly Free by *Freedom in the World*, demonstrating the extent to which both entrenched and aspiring authoritarian leaders rely on information controls to retain power. It is during perilous moments of political transition and possible transformation—such as protests, elections, and conflicts—that censorship of foreign information tends to intensify.

Blocking access to international websites, social media platforms, or the internet as a whole

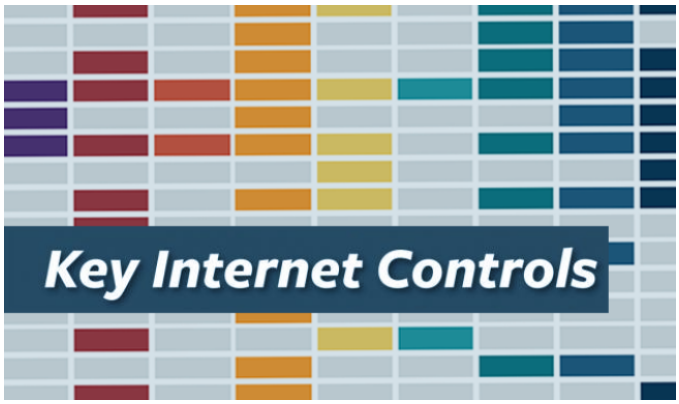
Authorities increasingly cut off domestic users from websites and social media platforms that serve international audiences. These national restrictions have a global impact, limiting connections to family members in other countries and the diaspora communities that use digital technologies to stay in touch with their countries of origin.

Since the February 2021 coup, Myanmar's military junta has cultivated a domestic intranet to help silence opposition to its takeover and consolidate its power. Residents can only access an estimated 1,200 websites and platforms through mobile connections. Facebook and Twitter—both popular

with anticoup protesters and key tools for communicating with allies abroad—remain inaccessible. The junta has also imposed shutdowns of internet service in towns across the country, often coinciding with military offensives against ethnic militias, armed prodemocracy groups, or communities that are suspected of supporting them. In practice, these restrictions have limited the sharing of evidence of human rights abuses with external audiences, forced residents to rely on military-dominated information sources, and helped to contain civic mobilization and dissent.

In Ethiopia, internet access has been restricted in the Tigray Region since November 2020, when armed conflict broke out between the federal government and forces associated with the Tigrayan People's Liberation Front. The shutdown has prevented people in Tigray from sharing their stories and reporting on actions by combatants that human rights groups have described as mass atrocity crimes, limiting opportunities for accountability and global solidarity. Similarly in July 2021, as Cubans mobilized the largest antigovernment demonstrations in the country since the 1959 revolution, the authorities briefly restricted internet access and blocked WhatsApp, Telegram, and Signal. These steps prevented protesters from effectively using digital tools to coordinate protests, and they separated the movement from independent news outlets and Cubans based abroad, who had rallied support for the demonstrations on international social media platforms.

While the vast majority of governments that limited access to foreign content did so to maintain their own power or thwart accountability, a notable exception came from the EU. Brussels ordered each member state's telecommunications providers to block the websites of the Russian state media services RT and Sputnik. These sites certainly promote incendiary and false content, and international human rights standards permit limits on free expression under specific circumstances including armed conflict. However, the EU's broad ban restricted all content from these sites rather than more narrow information related to the war. It also lacked clear sunset provisions and was imposed without adequate oversight, transparency, and consultation with civil society and telecommunications companies. The EU's insufficient clarity and specificity left companies scrambling to determine how to comply, leading to uneven blocking among member states. Furthermore, the ban set a flawed precedent for how democracies could respond to problematic information disseminated by other foreign state-owned news outlets, such as those based in Beijing.



Key Internet Controls

To track the different ways in which governments seek to dominate the digital sphere, Freedom House monitors their application of nine Key Internet Controls. The resulting data reveal trends in the expansion and diversification of these constraints on internet freedom.

Learn More ›

Targeting circumvention technology

Journalists, activists, and ordinary users in many countries have flocked to circumvention tools like virtual private networks (VPNs), which allow them to use the internet safely and anonymously while bypassing some forms of state censorship. In response, governments are increasingly blocking, criminalizing, or imposing regulatory requirements on the circumvention tools themselves.

Blocks on circumvention technology escalated in moments of political tension during the coverage period, when access to the uncensored international internet would have boosted those seeking to change the balance of power. During Venezuela's November 2021 regional elections, in which opposition parties sought to challenge the authoritarian rule of Nicolás Maduro, service providers blocked VPNs and the anonymous web browser Tor, presumably on government orders, in addition to widespread blocking of international and independent Venezuelan media sites. Venezuelan internet users were cut off from critical information, particularly the reports of foreign media and election-monitoring groups.

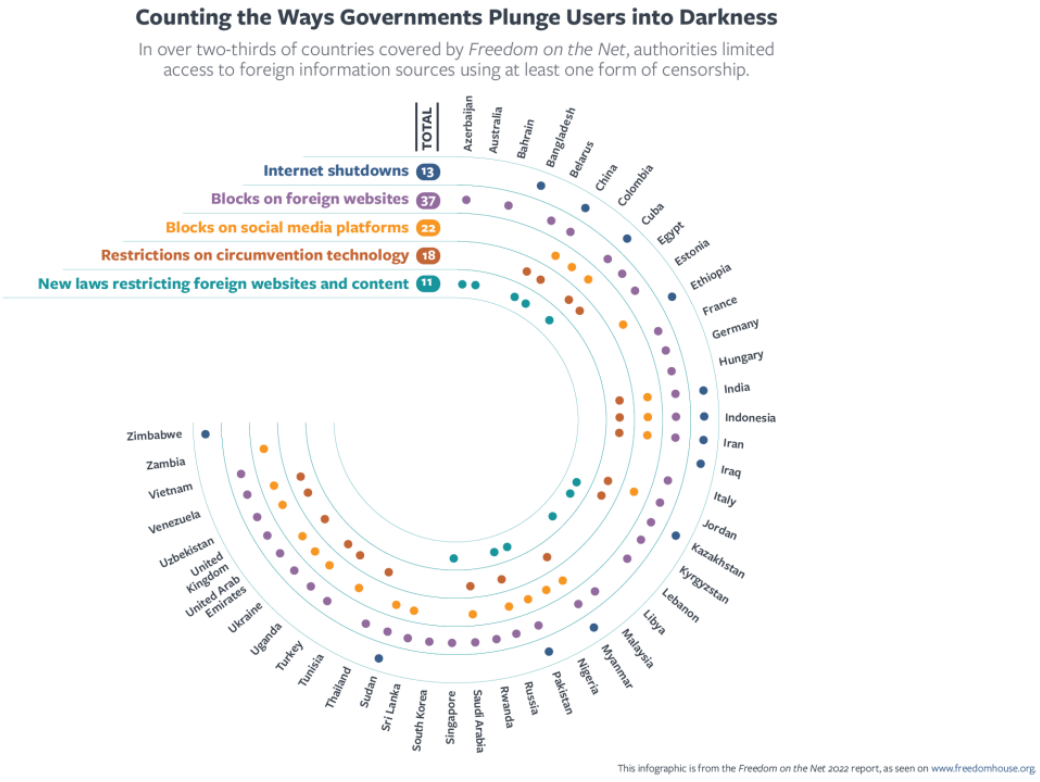
In India, new regulatory requirements for VPN providers were introduced amid government censorship demands targeting US-based technology companies as well as a two-year block on communications platforms owned by China-based companies, including TikTok and WeChat. The VPN services will be required to maintain subscriber records, such as names and IP (internet protocol) addresses, for five years and furnish them to the government on request, with steep fines for noncompliance. International providers TunnelBear and Norton have since made their services unavailable in India. In nearby Myanmar, security officials have reportedly employed cruder tactics to deter people from using the technology: they have arbitrarily searched civilians' phones for evidence of VPNs, detaining individuals who are found to have downloaded them.

Exploiting fears of foreign interference to inhibit independent media

Authorities also invoked the specter of foreign interference to expand censorship of websites based abroad or those that receive foreign funding. Website owners or journalists living outside a given country often have more leeway to resist government pressure and produce unfettered reporting. By requiring websites and related companies to be based domestically or to accept only domestic funding, a state can enhance its capacity to control the local information space.

In October 2021, Singapore's government added the Foreign Interference (Countermeasures) Act (FICA) to its formidable arsenal of censorship powers. In the name of preventing foreign meddling in domestic politics, FICA authorizes officials to block websites and order social media companies and other sites to remove speech if they suspect that the content in question was influenced by a foreign actor. A regulatory body suspended the license of the citizen news site *The Online Citizen* within a day of the bill's introduction in Parliament, citing concerns about foreign funding.

A restrictive Azerbaijani media law that was adopted in February 2022 limits the foreign funding that media—defined broadly to include both news outlets and individuals—can accept and requires media operators to be based in the country. The law further clamped down on what was already a tightly controlled online media environment, with many Azerbaijani journalists forced to operate from abroad to avoid state persecution.



Propping up state-aligned and state-owned alternatives to international platforms

Even as they increased pressure on foreign platforms over the past year, many repressive governments promoted pliant domestic alternatives as part of a strategy to create a siloed and

politically tamed information environment. If users migrate to state-aligned platforms, the domestic political costs of blocking international services would be reduced, facilitating further fragmentation.

In China, the government has been fairly successful in pairing systematic censorship of foreign services with robust investment in domestic platforms that are beholden to the ruling party. A more diverse social media market, including the development of smaller and more local platforms that meet the needs of a particular community, is sorely needed around the world. But companies owned by or with close ties to authoritarian governments are more likely to censor unfavorable content and become vehicles for state disinformation than their counterparts based in more democratic contexts. These so-called parallel platforms are often less transparent in their operations and policies, and they may be better shielded from civil society advocacy, media investigations, and other forms of public scrutiny.

Moscow's strategy to reduce reliance on foreign social media companies includes a requirement that mobile phones carry preloaded domestic apps. Following the invasion of Ukraine in February 2022, blocks on Facebook, Twitter, and Instagram drove users to VK and Odnoklassniki, both run by a parent company that is partly owned by Kremlin allies. Yandex, a popular Russian search engine and rival of Google, reportedly prioritized disinformation narratives and downgraded the search results for sites that criticized the invasion. In 2022, in a bid to win larger user bases for Russian platforms, authorities reportedly offered influencers monthly payments if they switched to RuTube and Yappy, in lieu of YouTube and TikTok, and toed the government's editorial line.

The push toward domestic platforms often followed explicit or implicit attacks on the credibility of international platforms, further undermining trust in the global information space. In Turkey, many state agencies flocked to the WhatsApp alternative BiP in 2021, after the Meta-owned app introduced a problematic privacy policy update. BiP is owned by the mobile operator Turkcell, which the state's sovereign wealth fund controls. The platform has a growing user base in Bangladesh, Indonesia, Pakistan, and Bahrain.

Increasing barriers to the cross-border flow of user data

In at least 23 countries covered by *Freedom the Net*, laws that limit where and how personal data can flow were proposed or passed during the coverage period. The affected countries span the democratic spectrum, including examples that are ranked Free, Partly Free, and Not Free by *Freedom in the World*. The transfer of data across jurisdictions is central to the functioning of the global internet and benefits ordinary users, including by improving internet speeds, enabling companies to provide critical services worldwide, and allowing the storage of records in the most secure data centers available.

As policymakers impose necessary privacy laws that safeguard sensitive information from commercial abuse, they may unintentionally drive fragmentation by creating a barrier between their own countries and those without similar standards. The ensuing patchwork of regulations could incentivize companies, particularly newer or smaller services, to concentrate their growth in certain countries, resulting in less diverse online ecosystems for users elsewhere.

The EU's 2018 General Data Protection Regulation (GDPR) permits the transfer of personal data only to jurisdictions with a sufficient level of protection in place. As more governments pursue laws that appear to align with GDPR standards, some have buried problematic obligations that either mandate domestic data storage, feature blanket exceptions for national security or state actors without safeguards, or delegate increased decision-making power to politicized regulators—all of which renders users vulnerable to government abuse despite improvements pertaining to the use of personal data for commercial purposes. Such contradictory "data washing" measures ultimately fail to strengthen privacy and further fragment the internet.

In August 2021, the Chinese government passed a data protection law that regulates the commercial use of personal data, creating an important set of guarantees for the country's billion internet users. But the law does not restrict the government's misuse of data, and it mandates domestic data storage for some companies, opening the door to further state intrusion and exploitation and imposing additional onerous barriers on the flow of personal data.

In Rwanda, a data protection law passed in October 2021 requires companies to store data in the country unless otherwise authorized by the country's cybersecurity regulator, rather than an independent data protection agency that is more insulated from law enforcement bodies. This localization clause leaves personal data vulnerable to abuse, particularly given that authorities have embedded agents in telecommunications companies for surveillance purposes and prosecuted dissidents based on their private messages.

Though modeled on the GDPR, the United Arab Emirates' new data protection law, in effect since January 2022, exempts government entities tasked with processing personal data from complying with baseline safeguards. While its constraints on commercial data access are welcome, the law

leaves the privacy of residents at risk: authorities in the country still have sweeping powers to monitor communications and seize data from service providers.

Breaking away from global infrastructure

Governments in at least seven countries, all of which are ranked Not Free in *Freedom in the World*, sought to centralize state control over domestic infrastructure and physically isolate their networks from the global internet during the coverage period. This form of fragmentation may be the least prevalent due to the exceptionally advanced technical and administrative capacities that it requires. It also entails considerable political will: infrastructural isolation presents economic costs to businesses operating domestically, can significantly slow down connection speeds, and deepens the risk to human rights. These challenges help explain why political leaders in countries with robust civic spaces, thriving technology sectors, and more pluralistic governance systems are less likely to impose such barriers.

The CCP and state-linked companies have cultivated the most sophisticated model of cyber isolation. Internet traffic from outside the country passes through centralized, state-controlled chokepoints, facilitating mass blocking, filtering, and surveillance. Following Beijing's path, the Iranian government has imposed state barriers between the local infrastructure and global traffic. In July 2021, authorities introduced the User Protection Bill to bolster the country's National Information Network, which has facilitated the restriction of access to international platforms and connections while directing users to domestic alternatives. The law would place the country's internet gateways under the authority of a working group that includes military and intelligence agencies.

The Russian government hastened its own progress toward infrastructural isolation over the past year. During a series of tests in June and July 2021, authorities claimed to have successfully separated the so-called RuNet from global connections, though technical experts remain skeptical. In April 2022, following his invasion of Ukraine, President Vladimir Putin appointed an interagency commission to pursue his goal of technical isolation.

The Cambodian government planned to route all international and domestic internet traffic through a single portal, dubbed the National Internet Gateway (NIG). This centralized chokepoint would allow authorities to censor content from around the world and surveil residents more easily. Cambodian officials unexpectedly delayed the NIG's implementation in February 2022, citing the COVID-19 pandemic and issues related to licensing and equipment installation. The decision came after extensive opposition to the NIG from the private sector, civil society, and experts at the United Nations.

The competition to control the web

Fragmentation at the national level is part of a global battle for control over the internet. Led by Beijing and Moscow, diplomats from authoritarian countries have promoted their model of cyber sovereignty at multilateral institutions. As secretary general of the ITU, China's Houlin Zhao encouraged a shift of control over the setting of technical standards away from multistakeholder bodies, where civil society and other nongovernmental experts have more sway, and toward the ITU itself, where only governments have input.

During Zhao's tenure, in 2019 and 2020, the Chinese telecommunications giant Huawei introduced the New IP proposal, a plan to fundamentally alter the interoperability of the global internet's infrastructure by redesigning common protocols to facilitate greater state control over domestic networks. While initially voted down by ITU members, rebranded elements of the proposal have since reemerged in standards-setting bodies. Chinese officials also launched in July 2022 the World Internet Conference International Organization in Beijing, intended to serve as a "shared" global community that would determine technical standards and governance. The organization, stemming from an annual meeting of the same name that was first held in 2014, could create a new forum in which the Chinese government can promote and incentivize other governments to adopt its authoritarian model of digital control.

BEIJING, CHINA - AUGUST 31: A screen shows secretary-general of the International Telecommunication Union Zhao Houlin speaking during the opening ceremony of 2021 World 5G Convention at Beijing Etrong International Exhibition & Convention Center on August 31, 2021 in Beijing, China. (Photo by VCG/VCG via Getty Images)

The Russian government has similarly leveraged international institutions to influence internet governance. At the United Nations in February 2022, negotiations began for a new cybercrime treaty, which was initially proposed by Russian diplomats and cosponsored by representatives from Belarus, Cambodia, China, North Korea, Myanmar, Nicaragua, and Venezuela—all ranked Not Free by *Freedom in the World*. Civil society has resoundingly condemned the proposed treaty as a new vector for digital repression. Moscow also joined Beijing in June 2021 to call for a more powerful ITU and endorse the right of each state to control its own "national segment of the internet." One Russian official explained the need for a more forceful version of the agency by claiming that the multistakeholder model of governance was "ineffective."

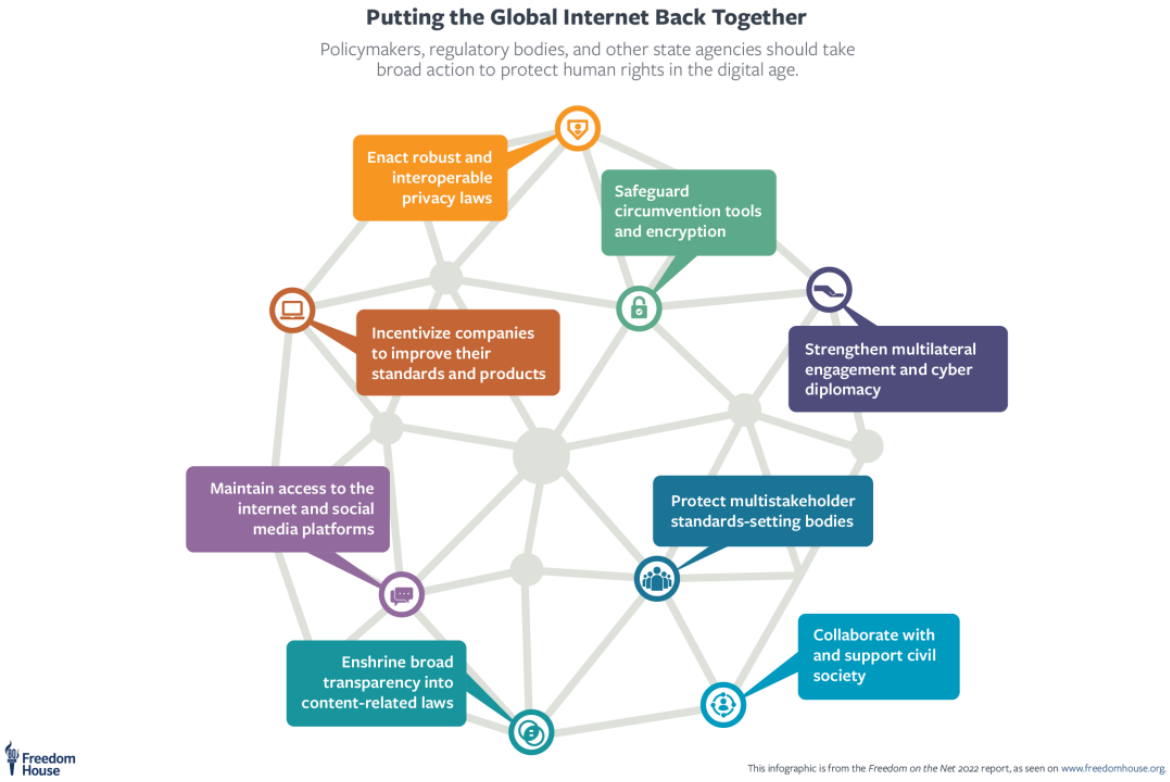
Democratic states step up globally

Some democratic leaders have revived efforts to shape global digital standards that uphold fundamental freedoms, creating a much-needed counterweight to authoritarian efforts. After allowing ITU secretary general Zhao to run unopposed in 2014 and 2018, Washington nominated Doreen Bogdan-Martin to seek the post, and she defeated a candidate backed by Moscow in a September 2022 vote by member states. Two US-led initiatives, the Summit for Democracy and the Declaration for the Future of the Internet, have sought to solidify common norms as a basis for further action. Moreover, the United States has pledged to strengthen and expand the Freedom Online Coalition in its upcoming role as chair in 2023.

Greater policy coordination among democracies is vital to the protection of a free and open internet.

Across the Atlantic, the EU and its member states have taken similar action. The Copenhagen Pledge on Tech and Democracy, led by the Danish government, uses a multistakeholder format by inviting governments, multilateral bodies, civil society, and the private sector together to protect human rights in the digital age. Separately, the EU's Digital Services Act (DSA) is a promising alternative to more censorial regulatory approaches and could serve as a global model. It strengthens transparency, limits advertising systems, and requires large platforms to provide data to independent researchers and organizations, which can then lead to more innovative and effective responses to online harms. The DSA also institutes a more inclusive coregulatory form of oversight and enforcement, including by using independent third-party auditors to review compliance, which can limit the risk of abuse.

However, the DSA framework features a problematic "notice-and-action" provision for companies to remove speech that is deemed illegal by EU authorities or member states, which could be abused to silence political, social, and religious speech. To limit this risk, Brussels and member states should clearly define and harmonize their definitions of what constitutes "illegal" speech in keeping with international law, and ensure that independent judicial authorities oversee any removal of content.



Harmonizing data protection to create a race to the top

Greater policy coordination among democracies is vital to the protection of a free and open internet. In a promising sign from April 2022, the governments of Canada, Japan, the Philippines, Singapore, South Korea, Taiwan, and the United States established the Global Cross-Border Privacy Rules Forum to bridge regulatory discrepancies and promote the free flow of data under what it determines as "best practices" for data protection. The EU and the United States also made progress during the coverage period following the European Court of Justice's invalidation of the EU-US Privacy Shield framework in 2020, a ruling that limited transatlantic data flows due to concerns about US national security surveillance programs. In March 2022, the transatlantic partners announced an agreement on Privacy Shield 2.0, set to be formalized in late 2022, that includes a redress mechanism for EU residents who are concerned about privacy violations as well as new privacy commitments by US intelligence agencies.

Governments also proposed, passed, or began enforcement of data protection laws that are compatible with rights-respecting provisions from existing international frameworks, a practice that can minimize the effects of fragmentation. South Africa's data protection law, which entered into full force in July 2021, was drafted to harmonize with parts of the GDPR, as was Sri Lanka's, which passed in March 2022. Both laws put limits on the transfer of personal data across borders except in certain cases, including transfers to a country with adequate safeguards. Protecting privacy does not necessarily require limiting the physical location of data storage. For instance, the proposed American Data Privacy and Protection Act in the United States avoids focusing on where data can be transferred and instead adopts a data minimization approach that limits what can be collected, how it can be stored, and with whom it can be shared.

Resisting internet fragmentation while protecting human rights

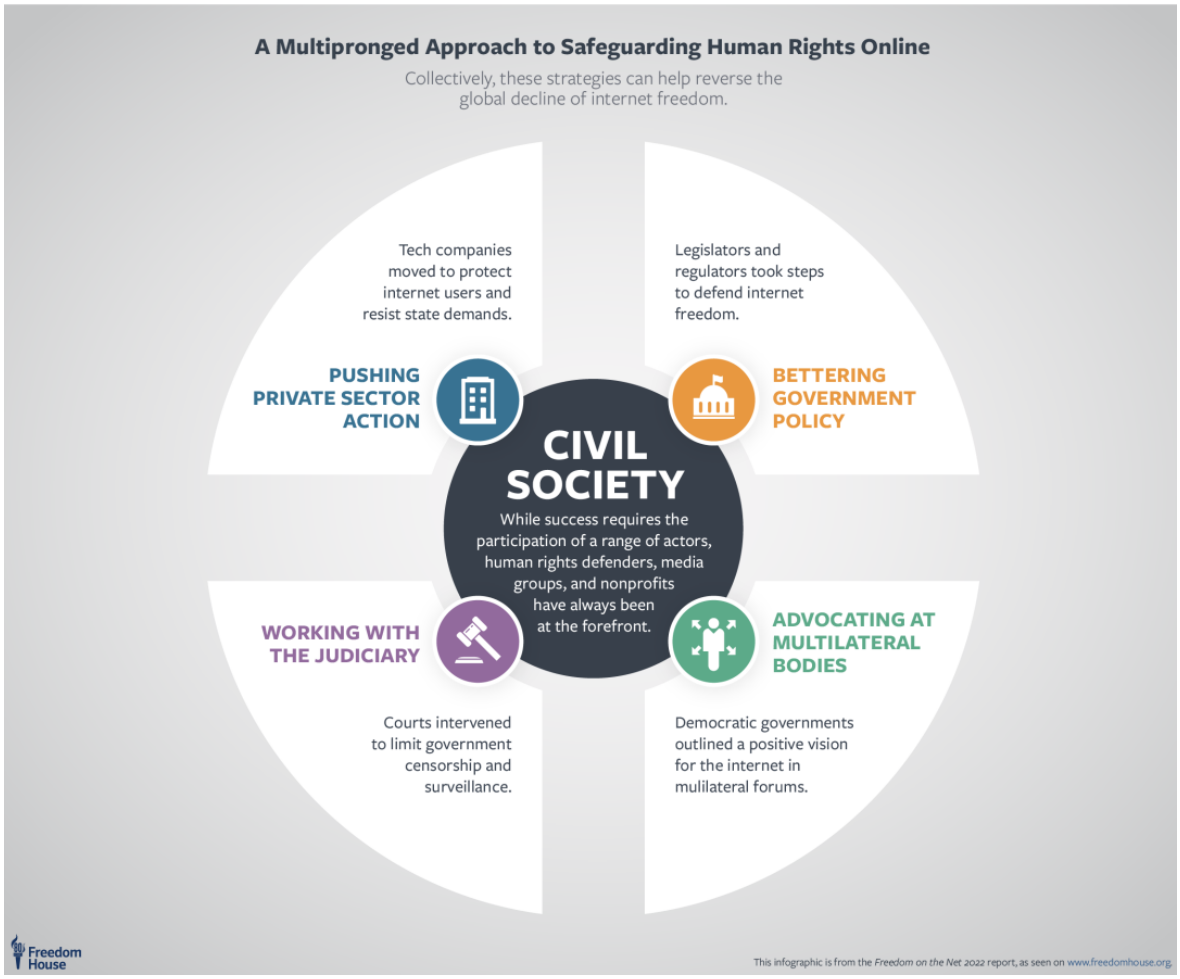
The values of human rights and open societies are mutually reinforcing. When implementing rights-protecting laws, governments should seek to reduce friction by coordinating their efforts across borders and aligning them with international frameworks whenever possible. Ultimately, democratic officials, technology companies, and global civil society groups should aim to empower individuals to play a greater role in making online spaces more free, secure, and inclusive. This is the best way to ensure that human rights are upheld in the digital age.

A Resilient Internet for a More Democratic Future

Twenty-six countries experienced net improvements in internet freedom over the past year, the highest such figure since the inception of *Freedom on the Net*. Though digital repression is undoubtedly becoming more sophisticated and entrenched into everyday life, responses from governments, civil society, and the private sector are beginning to yield results.

Freedom on the Net has identified proven strategies that marshal the structures, tools, and expertise necessary to prevent or address illiberal uses of technology by both domestic and foreign actors, as well as the broader societal harms that the internet often exacerbates. Some strategies provide short-term responses to instances of repression, while others build long-term mechanisms for accountability, governance, and oversight that can stave off the advance of authoritarianism over time. These approaches vary in effectiveness depending on a country's political context: building digital resilience in a backsliding democracy and doing so under an entrenched authoritarian regime involve different sets of challenges. Collectively, however, such efforts have the potential to reverse the global decline of internet freedom.

While success requires the participation of a range of actors, civil society has always been at the forefront. Nonprofit organizations, media groups, and human rights defenders with roots in a given country or region have played a leading role in first identifying and raising awareness of a problem, often tirelessly over years, and then creating a strategy to address it, with assistance from others who can organize the requisite financial and political resources. Governments, philanthropic foundations, private companies, and others with an interest in cultivating a free and open internet that works for all of its users should do their utmost to meaningfully engage with civil society groups that are involved in the fight against digital repression and internet fragmentation, providing funding, technical expertise, capacity building, and other support to advance their work.



Working with the judiciary

In at least 28 countries covered by this report, courts protected internet freedom. In many cases, problematic laws were struck down, creating precedents to guide future state actions. Court intervention appears to be the most effective at fighting censorship and surveillance in countries ranked Free or Partly Free by *Freedom in the World*, where judicial authorities remain independent from or somewhat resistant to political control. Efforts to protect internet freedom should prioritize strengthening the independence of courts and building their capacity to parse the legal and technical concepts that arise in cases involving human rights online.

In one positive example, the Zambian human rights organization Chapter One Foundation sued the country's communications regulator after it blocked social media platforms during the August 2021 presidential election. As a result of the legal action, the regulator signed a consent agreement, pledging not to act outside its legal authority and making a commitment to strengthen transparency regarding any future restrictions on telecommunications platforms.

In India, multiple civil society and media groups engaged in strategic litigation in response to the government's censorial Information Technology Rules, and in August 2021 a court halted the enforcement of problematic provisions in the regulations as part of a suit filed by an organization representing broadcasters. In a more recent case, Mexico's Supreme Court invalidated a biometric mobile-phone registry in April 2022, strengthening people's ability to communicate anonymously online. The decision came after civil society activists argued that the registry facilitated widespread surveillance, made personal data less secure, and contributed to social inequalities.

Pushing the private sector into action

In at least 30 countries over the past year, the private sector moved to protect internet freedom. In many cases, technology companies acted in response to civil society pressure, whistleblower testimony, and media scrutiny. Such cajoling can be necessary, as private-sector efforts to protect internet freedom have been inconsistent and affected by competing demands—including the mass collection of user data that forms the core business model of international social media platforms.

Following the Kremlin's invasion of Ukraine, tech companies scrambled to protect vulnerable users and avoid inadvertent support for a war of aggression. Google, Twitter, and Meta all limited the ability of Russian state media to monetize content across their platforms. They also rolled out new safety features to reduce online risks, such as Meta's expansion of end-to-end encryption for Instagram users in Russia and Ukraine and its introduction of ephemeral messages on the Messenger application for those in Ukraine. Twitter launched a Tor Onion service, allowing users in Russia to access the platform safely and anonymously after it was blocked by the government.

Under public pressure, social media companies have pushed back on the Indian government's efforts to increase control over online speech. After broad condemnation from civil society about its compliance with state censorship, Twitter resisted government orders to restrict content, including posts from Freedom House, before finally acquiescing in June 2022 after a company employee was threatened with criminal charges. Twitter then took the case to the judiciary, filing a lawsuit in July 2022 that could rein in the government's broad assertion of censorship powers.

The private sector has sometimes partnered with civil society, government actors, and academia to design innovative responses to online harms. In Taiwan, which faces a barrage of disinformation that can be traced to China, the popular Japan-based messaging application Line worked with civil society groups to develop a tool for users to report false information when it trends on the platform. The Taiwanese government launched a similar coordination effort following the Russian invasion of Ukraine, aiming to track war-related disinformation emanating from China.

Civil society has played a leading role in first raising awareness of a problem and then creating a strategy to address it.

Driving government policy changes to restore internet freedom

Policymakers, regulatory bodies, and other government agencies in at least 26 countries took steps to protect human rights online during the coverage period. These measures strengthened institutional safeguards for free expression, access to information, and privacy, and defended internet users from manipulative corporate practices. In some cases, government officials were reacting to targeted advocacy campaigns by civil society organizations; in others, their actions were an indirect outcome of long-term civil society efforts to shape the public discourse about policy and regulatory responses to disinformation, harassment, corporate malfeasance, and other harms online.

The Gambian government enacted legislation in July 2021 that affirmed a right to access public information, empowering journalists, civil society organizations, and ordinary citizens to hold the government accountable for its performance. The law was drafted using a multistakeholder model, with Gambian and international civil society and the private sector providing input.

In Armenia, domestic and international civil society groups combined public condemnation with private advocacy to persuade the government to repeal a criminal defamation clause that was originally passed in July 2021. The legislation, which criminalized serious insults of government officials and public figures, was invoked throughout the year to prosecute users who shared critical commentary, especially about Prime Minister Nikol Pashinyan. Civil society activists aired their concerns in private meetings with diplomats and in Armenian news outlets, and their objections were then cited in a formal appeal to the Constitutional Court. Government officials agreed to exclude the provision from a new criminal code that took effect in July 2022, and committed to broad consultation with nongovernmental groups when developing media-related laws in the future.

Civil society called on democratic policymakers to ensure that the sanctions they imposed in response to the Russian invasion of Ukraine did not impede critical internet access. In a March 2022 letter, more than 35 internet freedom groups and experts, including Freedom House, alerted President Biden to the dangers and unintended consequences of restricting internet services for users in Russia and Belarus. Weeks later, the Treasury Department exempted telecommunications services from US sanctions related to the invasion.

Independent regulators sought guidance from civil society and other experts on how best to prevent companies from undermining the rights of internet users. In August 2022, after the coverage period, the US Federal Trade Commission announced that it was accepting advice from the public about whether new rules were needed to protect US residents from corporate data collection. Such rules could allow the regulator to mitigate harms in the absence of comprehensive privacy protections under federal law.

NAIROBI, KENYA - 2022/08/15: Kenyans watch the announcement of the presidential results on the phone at the Gikomba market in Nairobi. The Independent Electoral and Boundaries Commission (IEBC) chairman declared Deputy President William Ruto the winner after a tight presidential race.

Progress on Internet Shutdowns

Internet shutdowns have long been a core tactic of digital repression. But this may be changing: the *Freedom on the Net* subscore pertaining to government restrictions on internet connectivity improved in 13 countries, the largest number of gains for a single indicator across the 21-question methodology this year. During the coverage period, governments in 14 of the 70 countries assessed shut off or throttled fixed or mobile internet services, compared with 20 countries in the report's 2021 edition and 22 in the 2020 edition. In countries where shutdowns continue to occur, they appear to be more localized and temporary, affecting fewer people for less time than past restrictions.

The trend suggests that a multipronged effort including strategic litigation, evidence-based research, multilateral and bilateral engagement, and targeted advocacy has helped to change the behavior of governments imposing shutdowns. For instance, researchers have illustrated that shutdowns take a toll on local economies, and they have been shown to correlate with higher levels of violence, undermining the argument that they are necessary to maintain peace and security. Lawsuits filed by

civil society groups, journalists, and others have led to judicial interventions against connectivity restrictions, most recently in India in 2022 and Sudan in 2021.

Disproportionate surveillance remains one of the most obvious problems affecting democracies' internet freedom performance.

Proactive advocacy aimed at both governments and internet service providers has succeeded in preventing possible shutdowns ahead of major events. For instance, members of the #KeepItOn coalition—comprising more than 280 civil society groups, including Freedom House, and led by the digital rights group Access Now—mobilized ahead of Kenya's general elections in August 2022 and Iraq's parliamentary elections in October 2021 to urge officials to maintain connectivity. Kenyan officials fulfilled their public commitments to refrain from restricting internet access, and no disruptions to internet access were reported in Iraq, unlike during the 2018 elections.

This sustained advocacy has contributed to a consensus at the multilateral level that shutdowns are unjustifiable and disproportionate. A UN report, commissioned by the Human Rights Council and released in 2022 to the General Assembly, incorporated civil society and private-sector input to outline recommendations on how to limit such censorship. The Freedom Online Coalition called for the immediate end of shutdowns in July 2021, launching an internet shutdown task force to design best practices for advocacy. The Group of Seven governments also publicly agreed in 2021 to cooperate in opposition to shutdowns when they are "politically motivated," although they reportedly softened their language after objections from the Indian government, a global leader in connectivity restrictions.

The path to stronger rights protections and a more resilient internet

The success of the collective effort against service shutdowns offers a model for tackling other critical problems that are driving digital repression and the fragmentation of the open internet. Strategies that build on the work of civil society to mobilize change in the courts, among governments, and at tech firms can yield better protections for human rights online on both a national and a global scale, particularly when they enlist multilateral and multistakeholder institutions. Without such campaigns, however, the internet is likely to grow more splintered, obstructing the exchange of diverse views and innovative ideas, constraining people's ability to organize for political and social causes, and severing cross-border connections between communities.

One advocacy effort has already identified its target: governments' purchase and deployment of intrusive commercial surveillance tools that violate the rights of internet users around the world. Technical researchers, human rights experts, and media investigations have recently documented the reach and abuses of the shadowy spyware industry, and governments have started to explore legal and regulatory restrictions on the sale of such products. These are welcome first steps, but more is needed.

Disproportionate surveillance remains one of the most obvious problems affecting democracies' internet freedom performance. Too often, rights considerations are disregarded in favor of the misguided belief that more intrusive tools and greater state access to data will necessarily contribute to a safer society. In addition to addressing the proliferation of spyware, democracies should impose robust controls on other forms of surveillance and protect end-to-end encryption, which limits the impact of such excessive monitoring. The coalition model for achieving digital resilience could be employed to focus much-needed public scrutiny on the question of which surveillance tools and practices are compatible with human rights. Such action would lay the groundwork for democracies to adopt rights-based regulations at home, clear the way for more coordinated and effective restrictions on the private surveillance market, and remove powerful and ever-evolving monitoring tools from the hands of abusive government actors, ultimately fostering a more democratic future.

Internet Freedom Score – Largest Declines