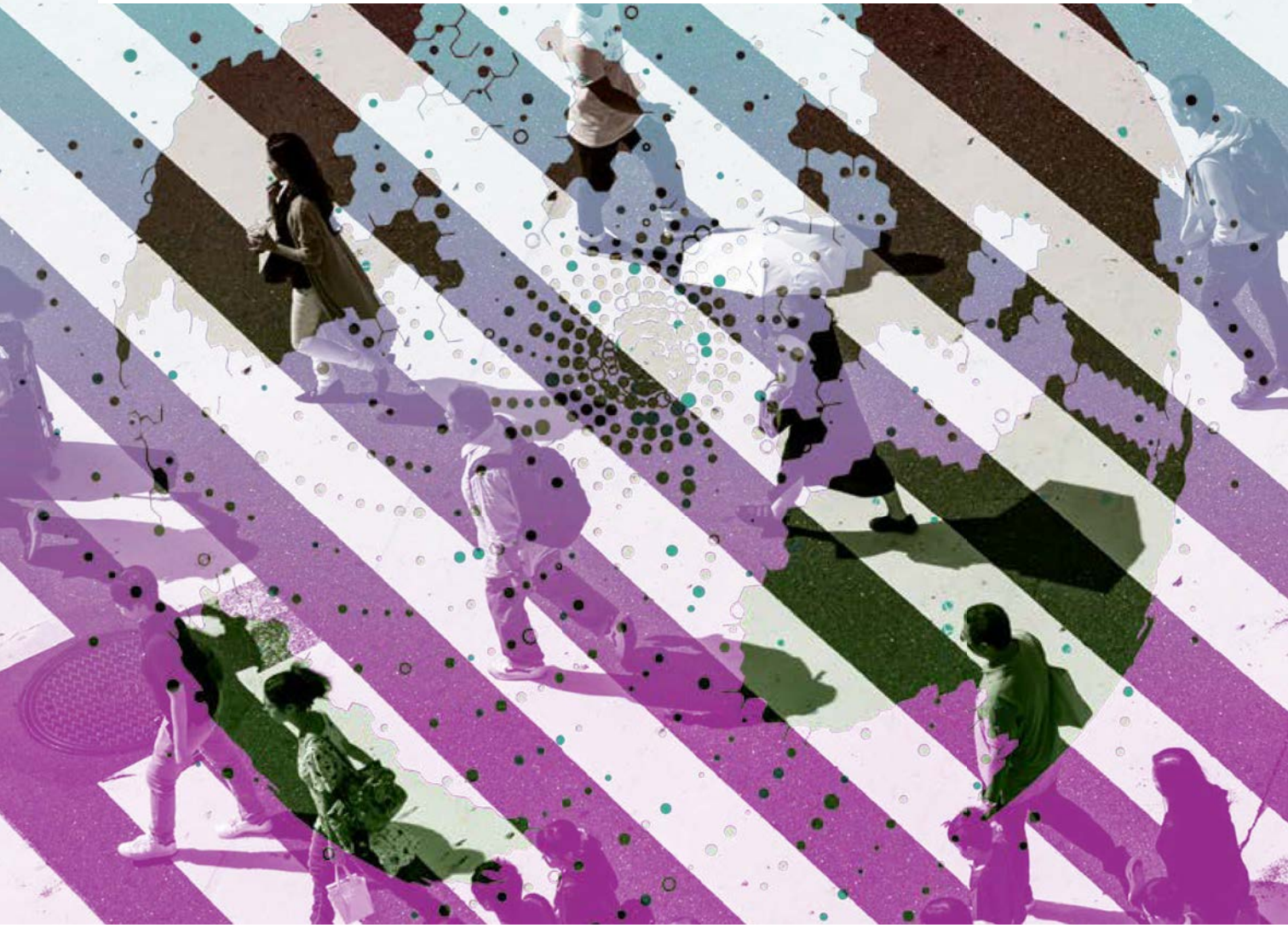
Tunnel Vision

Anti-censorship Tools, End-to-End Encryption,and the Fight for a Free and Open Internet



EUI EUROPEAN UNIVERSITY INSTITUTE

Freedom House

Funded by the European Union

Published by

European University Institute (EUI)

Via dei Roccettini 9, I-50014

San Domenico di Fiesole (FI)

Italy

ISBN:978-92-9466-674-1
doi:10.2870/8871367
QM-01-25-099-EN-N

www.eui.eu

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union.

Tunnel Vision

Anti-censorship Tools, End-to-End Encryption,and the Fight for a Free and Open Internet

By Grant Baker, Nils Berglund, Allie Funk, Patryk Pawlak, and Kian Vesteinsson

June 2025

Abbreviations

CDNs	Content Delivery Networks
CSAM	Child Sexual Abuse Material
DFI	Declaration for the Future of the Internet
DNS	Domain Name System
DPI	Deep Packet Inspection
EU	European Union
FOTN	Freedom on the Net
GDC	Global Digital Compact
IGF	Internet Governance Forum
IP	Internet Protocol
ISPs	Internet Service Providers
QUIC	Quick UDP Internet Connections
US	United States of America
TLS	Transport Layer Security
UK	United Kingdom
UN	United Nations
VPN	Virtual Private Network
WSIS	World Summit on the Information Society

Table of Contents

Key Findings 3

Introduction 5

A Less Free Internet 7

The Shifting of International Cyber Norms 10

Anti-censorship Tools in the Crosshairs 12

Blocking Anti-censorship Tools 14

Legal Restrictions on People's Ability to Use Anti-censorship Technology 17

Increasing VPNs' Burden to Operate in a Market 20

Pressuring App Stores to Remove Anti-censorship Tools from Marketplaces 23

End-to-end Encryption Under Pressure 26

Blocking and Criminalizing the Use of Encryption Tools 29

Compelled Decryption and Backdoor Pressure 30

Traceability Mandates 34

Debates Over Client-side Scanning 35

Policy Recommendations 38

Recommendations for Governments 39

Recommendations for the Private Sector 42

Glossary of Terms 45

About the Report and Methodology 48

Acknowledgements 50

About the Authors 52

01

Key Findings

- **Anti-censorship and end-to-end encryption technology power the free and open internet.** Anti-censorship tools, like virtual private networks (VPNs), encrypt and obfuscate internet traffic, enabling their users to access restricted political, social and religious content. End-to-end encryption protocols offer the highest degree of security for online communications. These technologies empower people to express themselves safely and securely online, strengthen national security and fuel the digital economy.
- **Restricting access to anti-censorship tools is a core authoritarian tactic of information control.** People's ability to use this technology to sidestep repressive censorship has driven autocrats to reduce access to these tools. Over the past five years, anti-censorship technologies were blocked in at least 21 of the 72 countries covered by the 2024 edition of Freedom House's *Freedom on the Net* (FOTN) report, all of which were ranked Not Free or Partly Free. Governments have also criminalized people's use of anti-censorship technology, placed onerous legal restrictions on VPNs' ability to operate in markets and forced app store providers to remove the tools from their marketplaces.
- **Governments' efforts to restrict end-to-end encryption technology are both blunt and subtle.** In at least 17 of the 72 countries covered by FOTN 2024, end-to-end encrypted services were blocked in the past five years. These blunt restrictions occurred in countries ranked Not Free or Partly Free, as part of states' efforts to increase access to personal data or prevent people from securely communicating. A broader set of governments, including in democracies, have obliged providers to decrypt communications, requested exceptional access to encrypted communications or sought to impose measures that do not overtly limit end-to-end encryption but would be impossible to implement without fundamentally breaking the cryptographic standards that enable it.
- **Investment and innovation are needed to strengthen digital resilience and defend the free and open internet.** Civil society, the private sector and several democracies have taken creative action to support access to anti-censorship and end-to-end encryption services. The private sector has increasingly integrated anti-censorship technology into widely used web protocols, while civil society organizations have aligned with policymakers to pass laws that protect end-to-end encryption. These efforts offer models for future action. Partnerships between policymakers, civil society, technical experts and the private sector can also help identify and implement proven and rights-based solutions to crime carried out over the internet, which has prompted disproportionate restrictions on anti-censorship and end-to-end encryption services in many countries.

02

Introduction

Governments around the world are increasingly exerting control over the technology that people depend on to access the free and open internet. In July 2024, thousands of Venezuelans flooded the streets to protest President Nicolás Maduro's fraudulent claims of victory in the July 2024 presidential election.[1] The government responded with a brutal crackdown, arresting and harassing political opponents[2] and blocking access to the end-to-end encrypted app Signal, the social media platform X and the websites of independent media and human rights groups.[3] These draconian efforts spurred a surge in people's use of anti-censorship technology. The VPN Proton became the most downloaded app in the country;[4] thousands of people also turned to Noticias sin Filtro, an anti-censorship app that provides access to a news feed of blocked media sites.[5]

In Venezuela and around the world, anti-censorship and encrypted tools are lifelines for resistance to and resilience over digital repression. These technologies create a zone of privacy for their users, enabling people to form and express opinions, communicate safely and securely, access independent reporting and mobilize for government and corporate accountability. These services also enhance cybersecurity, national security and economic growth, protecting government systems against foreign adversaries and companies against fraud.

The accessibility and effectiveness of anti-censorship and end-to-end encrypted tools depend on an internet that is free, open and interoperable. Anti-censorship tools allow people to bypass state censorship and communicate across borders. Just as encryption protocols underpin the functioning of the global internet by helping facilitate the secure transmission of data between websites, services that deploy end-to-end encryption provide stronger privacy guarantees, allowing people to trust the confidentiality of their communications.

This report examines increasing government restrictions on anti-censorship technology and end-to-end encryption, placing this trend within the broader deterioration of a free, open and interoperable internet. Many governments have attempted to clamp down on these tools through outright bans, formalized blocks and onerous legal requirements. The most repressive

1 Otis, J. and Kahn, C. (2024) Protesters take to the streets in Venezuela over contested presidential election.

2 PBS NewsHour (2024). World leaders voice concern as thousands arrested in Venezuela after disputed election.

3 El Nuevo País (2024). Venezuela bloquea Signal y X: Se intensifica la censura digital.

4 ProtonVPN (2024). The fight against censorship in 2024: how Venezuelans are using VPNs.; TechRadar (2024). 119 countries saw VPN usage soar in 2024 during times of political crisis.

5 TechRadar (2024). Don't call it a VPN: How a newsreader app seeks to revolutionize censorship circumvention.

measures are occurring exclusively in countries ranked Not Free and Partly Free in FOTN 2024. These restrictions have become a hallmark of autocrats' efforts to control the internet, act as a force multiplier for other forms of digital repression already prevalent in a given environment and reduce the ways in which people can bypass technical censorship and intrusive surveillance. Given the interconnected nature of the internet, efforts to undermine these tools in one jurisdiction have impacts far beyond those borders.

In contrast, democratic governments, civil society and the private sector have taken innovative action to support anti-censorship and end-to-end encrypted tools—an acknowledgement of how necessary this technology is for a free and open internet. Several governments have protected access to encryption under law and defended the technology's necessity for national security. The private sector has increasingly mainstreamed VPNs within their products, normalizing their use for everyday people. And civil society organizations have worked with legislators to drop alarming laws that introduce backdoors to encrypted communication.

To ensure the advancement of a free and open internet, this report offers concrete policy recommendations on how to sustain and build on this progress. Doing so is imperative for advancing the economic, societal and political benefits that the free and open internet engenders.

A Less Free Internet

Restrictions on anti-censorship technology and end-to-end encryption are part of a broader toolbox of techniques that have driven 14 consecutive years of decline in global internet freedom, according to FOTN.[6] In some of the most egregious cases, authorities disrupt internet access altogether. These internet shutdowns plunge whole communities into digital darkness, cutting off access to essential services like mobile payments, life-saving healthcare information and remote education. Many governments also pursue more targeted methods to censor the accessibility of specific forms of online content. In 2024, the FOTN report identified that at least 65 % of the world's 5.5 billion internet users[7] lived in countries where websites hosting political, social or religious content were blocked, an uptick from 56 % in 2020.[8]

---

6 Freedom House.

7 ITU (2024). Facts and Figures 2024.

8 Freedom House (2024). Freedom on the Net 2024: The Struggle for Trust Online.; Freedom House (2020). Freedom on the Net 2020: The Pandemic's Digital Shadow.

Authorities also have access to a booming private market for surveillance technology, enabling them to monitor the communications of journalists, activists and political opponents outside of the rule of law. According to the Carnegie Endowment for International Peace, between 2011 and 2023, at least 74 governments contracted with commercial firms to obtain spyware or digital forensics technology.[9] This growing capacity for advanced surveillance and increased access to data allows government actors with ill intentions to more easily harass, prosecute and even physically attack people, at home and abroad.[10]

Authoritarian regimes, whose leaders view the open internet as a threat to their political survival, deploy these repressive tactics systematically. For example, in each of the 21 countries ranked Not Free in FOTN 2024—in which some 35 % of the world's internet users reside—people were arrested for simply expressing their nonviolent views online.[11] In each of these countries, internet users also faced brutal violence, often state-sanctioned, in retaliation for their online activities. Many of these governments have also invested heavily in their technical capacity to implement advanced censorship and surveillance, allowing them to more seamlessly integrate digital repression into their governance systems.

The need to protect a free and open internet extends beyond authoritarian states and demands attention in more democratic contexts. Notably, 21 of the 27 countries that experienced declines in their overall score in FOTN 2024 ranked Partly Free or Free.[12] In 69 % of the countries FOTN ranked Partly Free or Free in 2024, internet users were arrested for their political, social or religious speech online. Governments in 43 % of these countries blocked websites hosting content protected under international human rights standards.[13]

---

9 Feldstein, S. and Kot, B. (2023). Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. Carnegie Endowment for International Peace.

10 Michaelsen, M. (2020). The Digital Transnational Repression Toolkit, and Its Silencing Effects. Freedom House; Anstis, S and Deibert, R. (2025). Silenced by Surveillance: The Impacts of Digital Transnational Repression on Journalists, Human Rights Defenders, and Dissidents in Exile. Knight First Amendment Institute.

11 See Background data.

12 Freedom House (2024). Freedom on the Net 2024: The Struggle for Trust Online.

13 See Background data.

WHY DOES THE FREE AND OPEN INTERNET MATTER?

The free, open and interoperable internet has brought immense political, economic and societal benefits to people and their countries.

HUMAN RIGHTS

A free and open internet enables the broad spectrum of human rights. It allows people to freely express themselves, access information from diverse sources, mobilize for shared causes across borders and safeguard their most intimate information.

DEMOCRATIC GOVERNANCE

Open access to the internet promotes greater transparency from governments and companies, enables broader public awareness of and participation in civic processes, and helps drive accountability for those in power. These conditions can improve public trust in and support the smooth operation of democracy.

NATIONAL SECURITY

The open internet allows governments to communicate securely, identify and share cybersecurity best practices, and collaborate on national security priorities. Technologies that underpin the open internet, including encryption protocols, protect government systems, data and intelligence from vulnerabilities that foreign adversaries exploit.

ECONOMIC GROWTH AND INNOVATION

The free and open internet has allowed companies of all sizes to operate globally and meet the needs of their customers, regardless of their location. The promise of economic growth is especially strong for countries in which digital transformation is expected to accelerate.

PUBLIC SAFETY

During times of conflict and other forms of crisis, access to a free and open internet is lifesaving. It facilitates the delivery of humanitarian aid, the dissemination of evacuation alerts and safety guidelines, and enhances first responders' ability to meet community needs.

The Shifting of International Cyber Norms

At the international level, the principles underpinning the free and open internet are being undermined by the rise of cyber sovereignty, the notion that the state should exert greater control over its domestic segment of the web. The most authoritarian leaders, who seek to align internet governance with their repressive agendas, have pursued a multi-pronged strategy to advance cyber sovereignty.[14] The Chinese government has leveraged a web of political and economic incentives in bilateral relations—including in trade agreements, investment ties and debt relationships—to engage other governments to adopt this more state-centric approach to regulating the internet.[15] Autocratic governments, including China's and Russia's, are also using the multilateral system, including agencies and bodies within the United Nations (UN) system, to cement a shift towards intergovernmental internet governance processes and away from the existing and dominant multi-stakeholder model.[16] This consensus-building approach, which incorporates diverse expertise from civil society, technical experts, academia, the private sector and government,[17] was essential to the development of the internet in its early days and its present-day operation, while enabling high standards of human rights protections.

Some democracies have also moved towards cyber sovereignty within their domestic policies, creating tensions with their efforts to protect a free and open internet. They often point to a range of concerns—including protecting national interests, managing cyber threats, competing with China's technological prowess and reducing dependencies on foreign tech markets—in doing so. Regardless of the justification, though, the impact remains: well-intentioned policies can still restrict the flow of data and information across borders and further silo the free and open internet on which human rights, economic growth and national security depend.

Governments' domestic policies sometimes contradict their stated international commitments. In the Declaration for the Future of the Internet (DFI), over 70 states committed to promoting a globally interconnected, open and secure internet grounded in respect for human rights and the multi-stakeholder governance model.[18] The Global Digital Compact, negotiated

[14] Funk, A. and Gorokhovskaia, Y. (2024). Authoritarians Are Hijacking Global Tech Cooperation to Undermine Human Rights. Freedom House.

[15] Tech Policy Press (2023). China's New UN Internet Proposal Could Resonate with Growing Economies.

[16] Komaitis, K. (2022). Protecting the Open Internet from China's Latest Governance Body. Brookings Institution.

[17] Freedom House (2022). Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet.

[18] European Commission (2022). EU and international partners put forward a Declaration for the Future of the Internet.

by all UN member states and opened for endorsements in 2024, outlines shared principles for digital cooperation that prioritize openness, inclusivity and human rights while explicitly committing to refrain from certain forms of digital repression, such as internet shutdowns.[19] The 2025 review process of the achievements of the World Summit on the Information Society (WSIS+20 Review Process) provides an opportunity for the international community to ensure that establishing a 'people-centered, inclusive and development-oriented information society' addresses the negative impact that digital repression has on the free, open and interoperable internet.[20]

Additionally, the fraying of transatlantic relations and a growing rift in technology policy between the United States (US) government and many of its European allies risk undermining joint progress made on advancing a free and open internet. Policy discrepancies over issues such as data protection have existed for years between the two markets. They have escalated under the current US administration, which has asserted that the European Union's (EU) approach to digital regulation unfairly targets US companies, creates barriers to growth in the American technology sector and stifles innovation, and has threatened retaliatory actions like investigations, tariffs and visa restrictions.[21] Certain US tech giants have also more closely aligned themselves with the US government's position,[22] which could reinforce concerns that non-European tech companies have unfair and outsized influence within Europe, and incentivize a sovereignty-based approach to governance.

A strong, international coalition that includes a robust and reliable transatlantic partnership is crucial in identifying shared solutions to the genuine challenges of the digital age, countering the rising influence of the world's digital authoritarians in bilateral and multilateral settings, and protecting the internet as a shared global resource for knowledge, dialogue, security and democratic advancement.

---

19 United Nations (2024). Global Digital Compact.

20 UNCTAD (2025). World Summit on the Information Society: 20-year review (WSIS+20).

21 The White House (2025). Fact Sheet: President Donald J. Trump Issues Directive to Prevent the Unfair Exploitation of American Innovation; Mukherjee, S. (2025). US FCC chair says EU Digital Services Act is threat to free speech. Reuters; Caulcutt, C. (2025). JD Vance warns Europe to go easy on tech regulation in major AI speech; US Department of State (2025). Announcement of a Visa Restriction Policy Targeting Foreign Nationals Who Censor Americans.

22 Bordelon, B. and Miller, G. (2025). After EU fines, Big Tech wants Trump to swoop in. Politico.

03

Anti-censorship Tools in the Crosshairs

Anti-censorship tools work by encrypting and obfuscating user internet traffic. These tools route a user's connection through servers located elsewhere, effectively creating a tunnel that masks the user's true location and allows them to access content blocked in their jurisdiction. Techniques like domain fronting, which leverage large cloud platforms to disguise a forbidden service's traffic under a permitted domain, are used to avoid censors. Tools like Psiphon[23] and Lantern,[24] both of which are free and open-source, layer traditional VPN capabilities with additional obfuscation and encryption methods. The Tor network[25] is a free, volunteer-run system that bounces internet traffic through multiple encrypted relays around the world to conceal users' location and provide them with access to censored content. Other tools that operate on a networked or peer-to-peer basis can offer people a means of getting online when governments initiate a shutdown.[26] Additionally, browsers, hosting providers and other companies part of the internet infrastructure ecosystem are increasingly incorporating VPNs or other censorship-resistant tools into their services.

When these tools are well constructed, privacy-preserving and meet the needs of the communities they serve, they provide people around the world with the means to bypass technical censorship and safeguard their personal data. But these benefits have put anti-censorship tools in the crosshairs of governments, particularly in contexts in which surveillance, censorship and other forms of digital repression are already widespread. Since as early as 2002,[27] the Chinese government—the pioneer in digital authoritarianism—has legally prohibited the use of VPNs to bypass censorship. Other governments have since followed suit, including Russia's, directly blocking them, criminalizing their use, placing onerous legal restrictions on their ability to operate or forcing digital marketplaces to remove them from app stores. Consequently, people have been left more vulnerable to state censorship and surveillance, and cut off from the benefits of a free and open internet.

Governments also impose restrictions due to the ways that anti-censorship tools can facilitate cybercrime or other illegal uses of the internet. Some companies, for example, offer web hosting services that are designed to support criminal activity through built-in VPNs. Some digital

[23] See https://psiphon.ca/

[24] See https://lantern.io/

[25] See https://www.torproject.org/

[26] See https://ceno.app/en/index.html

[27] Kalia, A and Galperin, E. (2017). Deciphering China's VPN Ban. Electronic Frontier Foundation.

marketplaces operating on the dark web also facilitate the sale of illegal drugs, sensitive personal information that has been stolen and other illegal items.[28] Concerns over how anti-censorship technology can allow people to access copyright-infringing content have also driven increased pressure on availability of these tools in some democracies. Restrictions that ban or otherwise limit access to anti-censorship tools jeopardize people's right to access information, online privacy and in certain cases, their safety. Law enforcement agencies have at their disposal more proportionate measures to tackle crimes carried out online. In February 2025, for example, the governments of Australia, the United Kingdom (UK), and the US sanctioned Zservers, a Russia-based bulletproof hosting provider[29], which supported websites engaging in criminal activity, including ransomware operations that stole millions of dollars from people globally.[30]

Blocking Anti-censorship Tools

As of March 2025, people in at least 21 of the 72 countries covered by FOTN 2024 had experienced blocks on anti-censorship tools in the past five years.[31] Governments restrict these tools through several techniques, including blocking Internet Protocol (IP) addresses of VPN services, restricting access to the ports circumvention tools use, using deep packet inspection technology (DPI) to recognize and block common VPN protocols—or employing a combination of these methods.[32] As certain VPNs rely on the same shared protocol, the latter method of protocol blocking can allow governments to block a wider range of tools simultaneously. The Chinese and Syrian governments deployed DPI technology to block VPNs as early as 2011,[33] and others, including those in Russia[34] and Egypt,[35] have deployed this method in recent years.

---

28 Spamhaus (2019). Bulletproof hosting – there's a new kid in town; US Department of Justice. (2024). Russian And Kazakhstani Men Indicted For Running Dark Web Criminal Marketplaces, Forums, And Trainings.

29 A term for web hosting services that offer VPN capabilities and other measures to help clients evade relevant legal requests.

30 Kovacs, E. (2025). 127 Servers of Bulletproof Hosting Service Zservers Seized by Dutch Police. Security Week.

31 See Background data.

32 NordVPN (2024). VPN bans: How they work and who's behind them.

33 Othman, D. (2013). Bypassing censorship by using obfsproxy and openVPN, SSH Tunnel.

34 Roskomsvoboda (2023). VPN in Russia: from blocking services to blocking protocols.

35 SMEX (2023). What is DPI Technology, and Why is Egypt Abusing It?

ANTI-CENSORSHIP TOOLS AND GOVERNMENT RESTRICTIONS

VPN

VPNs enable access to blocked news sites, social media platforms and global services. A VPN encrypts and routes internet traffic through an external server, masking a user's real location.

ANONYMITY NETWORK

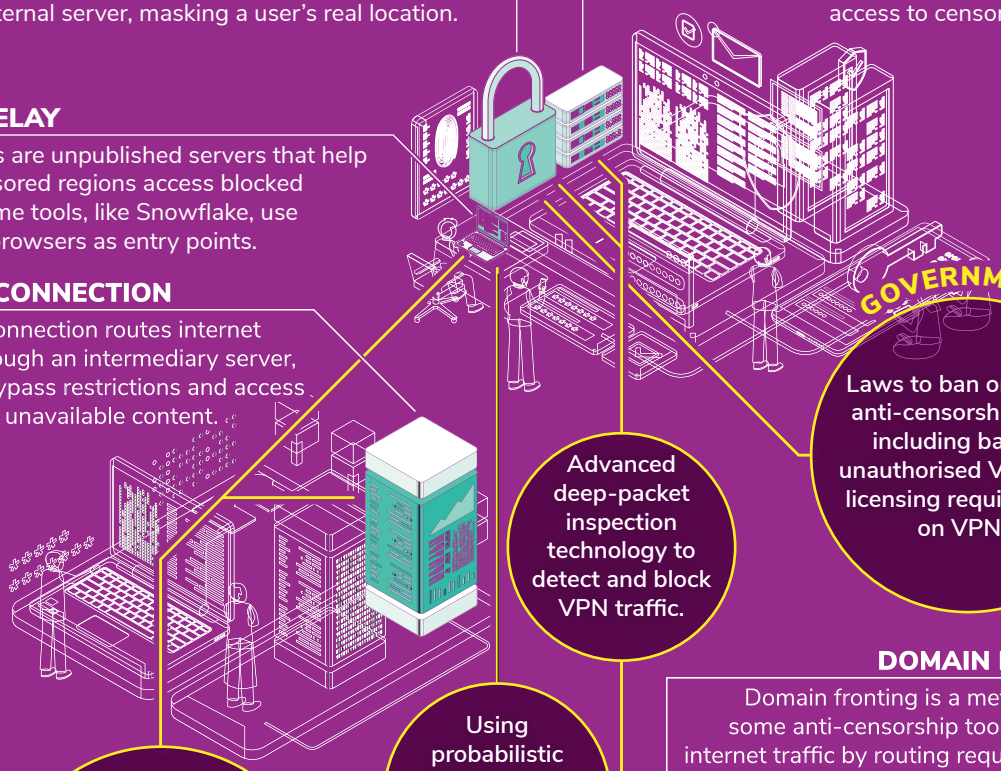
Anonymity networks like Tor route traffic through multiple encrypted relays, each knowing only its next hop, to conceal a user's identity and enable access to censored content.

BRIDGE RELAY

Bridge relays are unpublished servers that help users in censored regions access blocked services. Some tools, like Snowflake, use volunteers' browsers as entry points.

PROXY CONNECTION

A proxy connection routes internet traffic through an intermediary server, often to bypass restrictions and access otherwise unavailable content.



GOVERNMENT RESTRICTIONS

Laws to ban or control anti-censorship tools, including bans on unauthorised VPNs and licensing requirements on VPNs.

Advanced deep-packet inspection technology to detect and block VPN traffic.

DOMAIN FRONTING

Domain fronting is a method used by some anti-censorship tools to disguise internet traffic by routing requests through permitted domains, making it difficult for censors to identify and block them.

Using probabilistic algorithms to identify obfuscated traffic.

Blocking of specific content and websites. Authoritarian governments may blacklist the IP addresses or domains of known proxy servers or websites.

Detection and blockage of domain-fronted traffic patterns or ban of the front domains once they are discovered.

TRAFFIC 'CAMOUFLAGE'

Traffic obfuscation techniques modify internet traffic's appearance to make censorship tools less likely to detect or block VPNs, Tor or other circumvention methods.

In the most advanced censorship regimes, active scanning techniques—also referred to as active probing—identify circumvention tools' IP addresses and ports and proactively block them.[36]

In Myanmar, the military junta has restricted VPNs to reinforce its egregious censorship system. After taking power in a deadly coup in 2021, the military blocked news sites, Facebook, Instagram, WhatsApp and other popular platforms, and introduced a white-listing system that left mobile internet users with access to only some 1 200 websites.[37] Anti-censorship tools served as a lifeline for people to access independent information, communicate with each other and those abroad and go about their daily lives. In May 2024, the military deployed a new firewall with DPI capability to block a slew of prominent VPNs. The blocks reduced people's ability to reach educational institutions, health services, civil society organizations and businesses, according to research from Human Rights Myanmar.[38]

In Uganda, President Yoweri Museveni's government ordered the blocking of over 100 VPNs after first blocking major social media and messaging applications around the country's January 2021 general elections. The orders for VPN blocks came only two days prior to balloting and were followed by a five-day internet shutdown, preventing voters from expressing their views about candidates online and accessing information about the election.[39]

While VPNs are the most frequent targets of government-ordered blocking because of their useability and accessibility, governments have also blocked other anti-censorship tools. The Chinese, Iranian and Russian governments have restricted access to the Tor browser. In 2021, the Chinese government blocked proxy connections associated with Shadowsocks, a protocol that masks internet traffic to evade censorship, leading researchers to conclude that the Great Firewall's blocking capabilities had been adapted to target the seemingly random traffic many anti-censorship tools depend on.[40]

---

36 Ensafi et al. (2015). Examining How the Great Firewall Discovers Hidden Circumvention Servers. Association for Computing Machinery.

37 Psiphon Blog (2021). Shutdown in Myanmar: A Fresh Story with Old Challenges.

38 Human Rights Myanmar (2024). The Great Firewall of Myanmar.

39 Christopher, K. (2022). Investigating VPN Blocking and its Impact on Uganda's Preparations for the 2021 General Elections and Responses Afterward. Internews Optima.

40 Bock, K. et al. (2021). Exposing the Great Firewall's Dynamic Blocking of Fully Encrypted Traffic. OTF.

Developers of anti-censorship technology have innovated specifically to circumvent such blocks. A key area of innovation is efforts to make the tunnelling offered by these tools indistinguishable from standard web traffic, which has aided users in bypassing restrictions. In 2024, Tor launched WebTunnels, a tunnel that resembles standard internet traffic while offering users the same protection as a standard Tor connection. The Internet Engineering Task Force's MASQUE protocol suite integrates tunnelling over widely used Quick UDP Internet Connections (QUIC) and Transport Layer Security (TLS) protocols, providing another avenue for users to bypass the blocking of other anti-censorship tools.[41] While none of these methods are a panacea to governments' increasing sophistication for censorship, they continue to increase the cost of restrictions and limit their effectiveness.

Legal Restrictions on People's Ability to Use Anti-censorship Technology

Alongside blocking, some governments have directly criminalized the use or promotion of anti-censorship technology. These laws often deploy broad, vague language, incentivizing people to avoid downloading or using anti-censorship tools out of fear of repercussions.

In August 2023, the Jordanian government enacted a cybercrime law introducing criminal penalties for using anti-censorship tools for overly broad 'criminal' purposes, including criticism of the monarchy or harming the country's relations with foreign states.[42] This measure followed a surge in VPN usage in 2023 after the government blocked TikTok amidst mass protests over rising petrol prices.[43] In Tanzania, where homosexuality is illegal and LGBTQ+ websites are blocked, an October 2023 measure stipulates that people who do not inform the Tanzania Communications Regulatory Authority (THRA) about their VPN use face a minimum of two years in prison or a fine of 5 million Tanzanian shillings (EUR 1 780). Several gay men noted this measure effectively restricted their ability to use VPNs due to fear of government reprisal.[44]

---

41 See https://datatracker.ietf.org/wg/masque/about/

42 Holleis, J (2023). Jordan: Cybercrime law slams free speech as criminal content. DW; Amnesty International (2024). Jordan: New Cybercrimes Law stifling freedom of expression one year on.

43 Roya News (2025). Amazon makes last-minute bid for TikTok as US ban deadline approaches.

44 Minority Africa (2024). Tanzania's new VPN policy leaves LGBTQ+ individuals exposed.

HOW A VPN BYPASSES CENSORSHIP

Two people are based in the same country, and both want to access a news website blocked by the government.

WITH VPN

WITHOUT VPN

Establish a secure tunnel between the user's device and the VPN server.

DNS SERVER

ENCRYPTED TUNNEL
The user's online activity is hidden from censors.

Encrypt data

VULNERABLE TO CENSORSHIP
Governments and ISPs can monitor users and block websites using a range of methods, including IP blocking, DNS blocking and Deep Packet Inspection.

VPN SERVER
Connects the user to the open internet as if they were in a different location.

Masks user's IP address, so it appears as if their internet activity is coming from the VPN server.

BLOCKED SITE
Access denied. User sees an error, redirection or blank page.

OPEN, GLOBAL INTERNET
Website accessed

The user's internet traffic is routed through the VPN server.

Autocratic governments have discouraged the use of tools they deem unauthorized, while promoting their preferred alternatives. In Iran, one of the world's most hostile environments for internet freedom, the government prohibited unsanctioned VPN use in February 2024. The law, which does not assign criminal penalties to the prohibition, provides an exception for people who obtained government approval.[45] Domestic VPN companies have since flourished, prompting analysts, including members of the Iranian parliament, [46] to speculate that the industry benefits from government ties. Many Iranian VPN websites are not restricted by the country's extensive blocking regime, and one Iranian former cybersecurity official noted that authorities have access to extensive data from VPN companies,[47] suggesting that intelligence agencies may benefit from their wide use. The ascendance of state-linked VPNs, at the expense of independent and secure anti-censorship tools, puts Iranians more at risk of state repression and limits their ability to access uncensored information from the global internet.[48]

Employing a similar tactic of supporting specific VPNs, the Russian government reportedly spent 14 billion roubles (EUR 152 380 000) on state-approved VPNs in 2024, as state institutions and private entities rely on these tools primarily to circumvent sanctions.[49] For ordinary users and the media, however, the mere discussion of VPNs is criminalized. A law banning the promotion or use of banned VPNs took effect in March 2024, just ahead of a sham presidential election that kept President Vladmir Putin in power for his fifth term.[50] The law encompasses discussions of advertisements for VPNs, guides on how to use them and recommendations for what the government claims are the most secure VPNs. A July 2024 amendment expanded the definition further to include scientific and technical information about these tools. This repressive law, coupled with the widespread blocking of VPNs, effectively compels people to use low-quality or state-endorsed VPNs.[51]

People have also faced arrest or fines for using anti-censorship tools. Mehmut Memtimin, a Uyghur student arrested by Chinese authorities in 2017, was sentenced to 13 years in prison for

[45] Dehshiri, A. (2024). The use of VPNs is prohibited, but not criminalized. Filter Watch.

[46] Donya-e-Eqtesad (2025).

[47] Salami, M. (2023). Internet Filtering in Iran Boosts VPN Business – Much of it Government-Owned. Stimson.

[48] WANA News (2025). The Shadow Economy of VPNs in Iran.

[49] Baker, G. (2024). Another Door Closes: Authoritarians Expand Restrictions on Virtual Private Networks. Freedom House.

[50] Chiu, L. (2024). Russia Implements Ban on VPN Advertisement Ahead of Presidential Election. Kyiv Post.

[51] Roskomsvoboda (2024).

using a VPN to access 'illegal information'.[52] In May 2025, several people in India's Jammu and Kashmir region were detained and face up to a year in prison for allegedly violating a two-month ban on the use of VPNs.[53] The prohibition was issued by district authorities after a terrorist attack in the region and an ensuing conflict between India and Pakistan. Indian federal authorities also ordered the geo-blocking of news sites and the social media accounts of Indian and Pakistani journalists.[54] Security forces in Myanmar also stopped people on the street and searched their phones for VPN applications, fining individuals found to have one installed.[55]

Increasing VPNs' Burden to Operate in a Market

Governments have also escalated their legal control over VPN providers, undermining the privacy and anti-censorship benefits that the tools provide to their users. Many new laws introduce requirements for companies to register, retain users' personal data, impose content restrictions that contradict international human rights standards or otherwise make it more onerous to operate in a particular jurisdiction. These requirements have grown standard for internet service providers (ISPs) and social media platforms. Applying obligations like data retention mandates to VPNs gives governments yet another intermediary from which to request people's intimate information. In some cases, these laws have incentivized VPNs to leave markets altogether.

In Pakistan, the government has leveraged VPN registration requirements to support its broader censorship of political, social and religious speech.[56] The Pakistan Telecommunication Authority (PTA) first introduced VPN registration requirements in 2010,[57] and has repeatedly sought to enforce them.[58] In August 2024, the PTA announced it had white-listed over 20 000

---

52 Radio Free Asia (2023). Uyghur university student serving 13-year sentence for using VPN.

53 Office of the District Magistrate Doda (2025). Ban/Prohibition on the use of Virtual Private Networks; Ali, J. (2025). 'Attack on Individual Freedom': Doda Police Detains VPN Users, Legal Experts Slam Move. The Wire; Order issued under BNSS sec 163; criminal penalties under BNS sec 223.

54 Pandey, K. (2025). Digital Censorship After Terrorist Attack in Kashmir. Medianama.

55 Peck, G. (2024). Myanmar's embattled military government cracks down on free flow of news by blocking VPNs. AP News.

56 Freedom House (2024). Pakistan.

57 Castro, C. (2024). Has Pakistan begun the crackdown on 'unregistered' VPNs?. Tech Radar.

58 Shahbaz Butt, S. (2020). Problems with PTA's VPN Registration. Bolo Bhi.

registered VPNs, though it did not name them.[59] Some government officials called for the PTA to block unregistered anti-censorship tools, saying they are used for violence and 'access [to] pornographic and blasphemous content'.[60] In November 2024, Pakistanis reported difficulty accessing services like VPN Unlimited and TunnelBear.[61]

VPN companies have chosen to close servers or leave markets in the face of onerous legal obligations that threaten user privacy. In 2020, the no-log VPN provider Private Internet Access shut down and wiped its servers in Hong Kong after Chinese authorities imposed the draconian National Security Law, which allows law enforcement to carry out the warrantless seizure of servers.[62] In April 2022, India's cybersecurity agency ordered all cloud service providers to log users' personal information on their servers and store that information for up to five years.[63] The agency has issued compliance notices under the 2022 order but refused to disclose information about their nature.[64] Several VPN companies argued such a measure would be impossible, and many providers pulled their servers out of the country or stopped offering their services in India, leaving people with less reliable options for securely browsing the internet.

Some democratic policymakers have also increased legal obligations on VPN providers over concerns around access to copyright-infringing content. In February 2025, the Italian government introduced new obligations under its existing Piracy Shield framework to require VPNs and Domain Name System (DNS) resolvers to block illegal streaming of live events within 30 minutes.[65] This extremely short time frame and the law's IP address blocking mechanism provide intermediaries like VPNs with limited time to verify that blocking requests are

[59] Aaj News (2024). PTA whitelists 20,437 VPNs as part of regulation initiative.

[60] Ali, U. and Ali, K. (2024). Interior Ministry demands VPNs blockage, claims it is used by 'terrorists to facilitate violent activities'. Dawn.

[61] Aaj News (2024). PTA whitelists 20,437 VPNs as part of regulation initiative; Ahmed Shaikh, M. (2024). Reports emerge of nationwide VPN access 'restrictions, throttling'. Dawn.

[62] Private Internet Access (2025). Private Internet Access shuts down VPN servers in Hong Kong due to new national security law.

[63] Scroll (2022). India orders VPN service providers to collect user data or face jail term.

[64] Malhotra, G. (2023). Top Secret: One year on, CERT-In refuses to reveal information about compliance notices issued under its 2022 Directions on cybersecurity. Internet Freedom Foundation.

[65] Castro, C. (2025). 'Network blocking is never going to be the solution' – Cloudflare slams anti-piracy tactics. Tech Radar.

DIGITAL REPRESSION IN RUSSIA

Escalation Timeline

2016

JULY

The government enacts the Yarovaya law, requiring encrypted online services to decrypt content or share the keys with service providers.

2017

JULY

A new law enables Roskomnadzor, the government censorship authority, to block VPNs that do not comply with the list of banned websites.

2018

APRIL

A Moscow court orders the blocking of Telegram because the messaging service refused to comply with the Yarovaya law.

2019

MAY

The introduction of the Sovereign Internet Law enables Roskomandzor to block content directly and establishes a plan for a Russian internet isolated from the rest of the world.

JUNE

Roskomnadzor sends direct orders to popular VPNs to comply with its list of banned websites or face blocking.

2021

JUNE-SEPTEMBER

The Kremlin begins blocking some of the most popular VPN services in the country.

2022

FEBRUARY

The Kremlin launches an illegal full-scale invasion of Ukraine.

FEBRUARY-MARCH

The government blocks access to popular social media platforms, driving a surge in the usage of anticensorship tools.

MARCH

A law banning the promotion or advertisement of VPNs comes into effect.

2024

JULY-SEPTEMBER

At least 98 VPN apps were unavailable in the Russian App Store; the majority (58) were removed by Apple during the summer at Roskomnadzor's request.

AUGUST

Roskomnadzor blocks Signal, claiming it facilitated terrorist activities.

targeting legitimately copyright-infringing content,[66] which raises the risk of lawful content accidentally being restricted.[67] The law's lack of judicial oversight over blocking decisions, and broad power provided to the country's regulatory agency, have also raised concerns about due process and effective avenues of appeal.

In France, Canal+, a television and over-the-top subscription video service, and the Ligue de Football Professional, the governing body that manages French professional football, opened a case at a Parisian court to force prominent VPNs to block copyrighted content.[68] The case follows a 2024 court decision in favour of Canal+ that ordered Cisco, Cloudflare and Google to block illegal streaming websites on their DNS resolvers. The VPN Trusted initiative has stated VPN providers could leave the country if ordered to block content.[69]

Rather than wholesale blocking and increased obligations on VPNs, a more proportionate approach to addressing copyright-infringing content would be narrower requirements for content removal, with strong judicial oversight and effective avenues of appeal. When democracies impose disproportionate blocking obligations on VPNs, they risk threatening access to privacy-preserving products that provide people's online activities and personal data with an additional layer of protection from corporate and government surveillance. It also sets a dangerous precedent that legitimizes the politicized pressure applied to VPNs by authoritarian regimes.

Pressuring App Stores to Remove Anti-censorship Tools from Marketplaces

Intermediaries, including digital marketplaces, also offer opportunities for governments to limit access to anti-censorship tools. Legal orders for app stores to remove VPNs from their

[66] Moody, G. (2025). Massive Expansion Of Italy's Piracy Shield Underway Despite Growing Criticism Of Its Flaws. Tech Dirt.

[67] Freedom House (2025). Italy; Masnick, M. (2024). Italy's 'Piracy Shield' Misfires, Blocks Google Drive In Anti-Piracy Blunder. Tech Dirt.

[68] Phillips, G. (2025). French broadcaster Canal+ launches sweeping attack on leading VPNs. Tom's Guide; Henshell, R. (2025). VPN providers may leave France under pressure from Canal+. The Connexion.

[69] Internet Infrastructure Coalition (2025). VPN Trust Initiative (VTI) Opposes Misguided Legal Effort to Extend Website Blocking to VPNs; Van der Sar, E. (2025). VPN Providers Consider Exiting France Over 'Dangerous' Blocking Demands. TorrentFreak.

marketplaces often come alongside efforts to block other services, or are issued after anti-censorship tool providers refuse to comply with repressive laws.

One of the first such cases to be publicly reported came in 2017, when Apple complied with a Chinese government demand to remove anti-censorship tools that allowed users to circumvent the so-called Great Firewall.[70] Such removal demands have since become more common. Between July and September 2024, Apple removed nearly 58 VPN applications from the App Store in Russia with no public explanation. In March and April 2025, Roskomnadzor, the Kremlin's internet regulator and censorship authority, issued takedown orders to Google targeting 212 VPN applications, under the March 2024 law that criminalizes the promotion of VPNs. These orders included apps that were already unavailable on Google's Russian Play Store. GreatFire's research found 53 VPN apps unavailable in Russia, but uncovered no evidence that Google complied with any of the 212 takedown requests issued by Roskomnadzor.[71]

More democratic governments have also taken steps to pressure app stores to remove access to this technology. In January 2025, Indian authorities ordered app stores to remove a dozen anti-censorship tools because they had not complied with the data retention requirements imposed in 2022.[72] Brazil's Supreme Court also briefly ordered app stores to remove VPNs in August 2024 as part of its order blocking the social media platform X.[73] Though the order was quickly rescinded, it sets a worrying precedent for the restriction of anti-censorship tools in more democratic contexts.

---

70 Roy Choudhury, S. (2017). Apple removes VPN apps in China as Beijing doubles down on censorship. CNBC.

71 GreatFire (2025). Russian Government Escalates War on VPNs and Censorship Circumvention Tools; GreatFire (2024). Unveiling the Extent of VPN App Removals by Apple from the Russia App Store: An Analysis of Silent Removals and the Need for Transparency. These figures were updated on June 27, 2025, after the publication of the report, based on feedback from GreatFire (Greatfire.org).

72 Times of India (2025). Apple and Google have removed these six VPN apps from app stores for failing to abide by India's data laws; Internet Freedom Foundation (2024). IFF/2025/002.

73 Poder360 (2024). Moraes volta atras sobre uso de VPN no Brasil.

THROWING AWAY THE KEY

Restrictions on end-to-end encrypted and anti-censorship tools

In at least 21 of the 72 countries

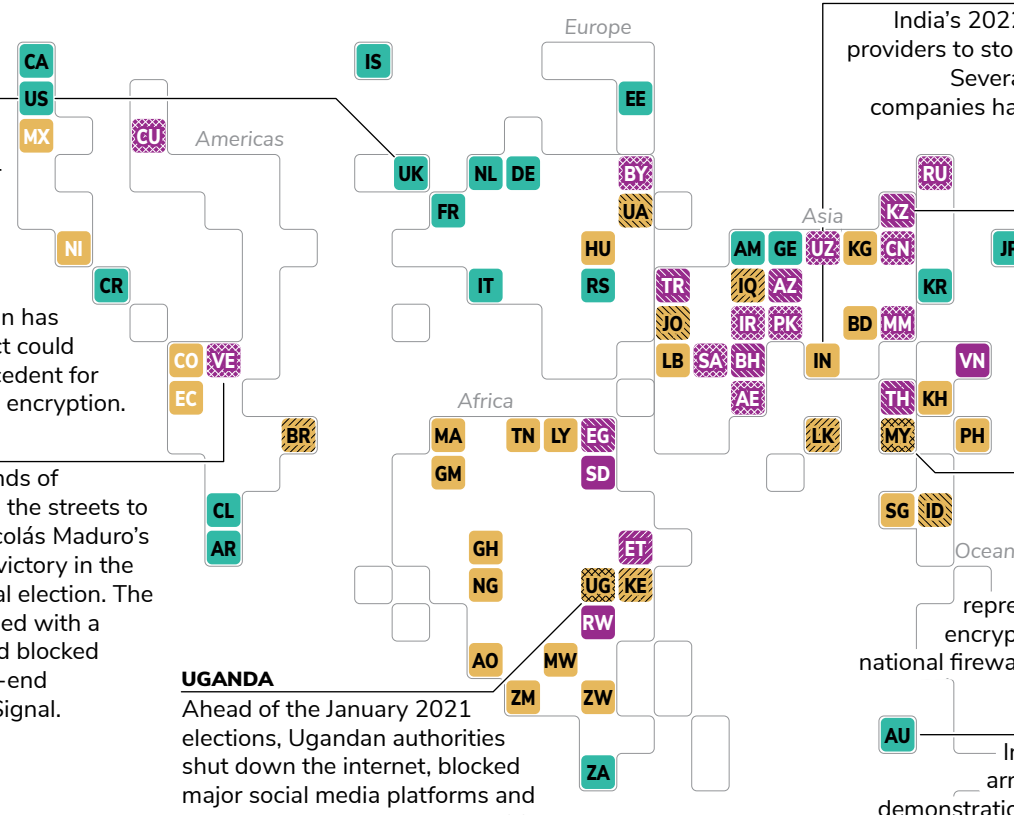
covered by FOTN 2024, anti-censorship tools were blocked in the past five years.

FOTN status
2024
Not Free | Partly Free | Free

Blocked
2020-2025
Anti-censorship tech | E2EE messaging platforms

In at least 17 of 72 countries

covered by FOTN 2024, end-to-end encrypted services were blocked in the past five years.



UNITED KINGDOM

The 2023 Online Safety Act granted regulators the power to compel platforms to scan private, encrypted messages for harmful content. While implementation has been delayed, the Act could set a dangerous precedent for breaking end-to-end encryption.

VENEZUELA

In July 2024, thousands of Venezuelans flooded the streets to protest President Nicolás Maduro's fraudulent claims of victory in the July 2024 presidential election. The government responded with a brutal crackdown and blocked access to the end-to-end encrypted platform Signal.

UGANDA

Ahead of the January 2021 elections, Ugandan authorities shut down the internet, blocked major social media platforms and ordered the blocking of over 100 VPNs, limiting people's ability to share information.

INDIA

India's 2022 regulation required VPN providers to store user data for five years. Several privacy-respecting VPN companies have shut down their Indian servers in response.

KAZAKHSTAN

As of June 2024, the websites for over 70 anti-censorship tools were blocked in Kazakhstan, making it much harder for people to access their services.

MYANMAR

Following the 2021 coup, Myanmar's military government ramped up digital repression, blocking VPNs and encrypted apps and rolling out a national firewall to monitor online traffic.

AUSTRALIA

In 2022, climate protesters arrested for an unauthorized demonstration were barred from using encrypted messaging apps as a bail condition, marking encryption use as inherently suspicious.

04

End-to-end Encryption Under Pressure

The security of the global internet has been bolstered by the widespread adoption and standardization of encryption protocols over the past 15 years, like TLS and QUIC. Building on this foundation, end-to-end encryption specifically has become a security best practice. End-to-end encryption refers to communication services in which only the sender and the intended receiver of a message have the cryptographic keys to open it—excluding the operator of the messaging service, ISPs and other intermediaries. The Signal app encrypts all content and metadata, making it one of the most secure platforms. Meta's WhatsApp and Apple's iMessage also encrypt the content of communications, although not communications metadata such as information about the sender and receiver.

End-to-end encryption is employed widely as a security measure in government operations. The US cybersecurity agency urged officials to 'use only end-to-end encrypted communications' in the aftermath of cyberattacks on telecommunications infrastructure in December 2024;[74] the European Parliament made a similar recommendation.[75]

The privacy and security provided by end-to-end encryption has long drawn the ire of governments. In some of the world's most repressive environments, end-to-end encryption services are blocked, or use is criminalized. A more diverse group of governments, including those with democratic systems, oblige providers to decrypt communications or permit officials to request exceptional access. Policymakers have also pursued more subtle measures that do not limit encryption outright but would be impossible to implement without fundamentally breaking the cryptographic standards that enable it, such as content governance laws that do not exempt end-to-end encrypted services from content removal mandates.

Governments have sought to break end-to-end encryption for a broad range of purposes, from accessing the communications of journalists to addressing terrorism, child sexual abuse and other serious crimes. However, restricting end-to-end encryption, regardless of the purpose, compromises its security benefits for all users. It undermines people's ability to maintain private communications, speak freely and safeguard their sensitive information, with potentially life-threatening consequences in authoritarian spaces.

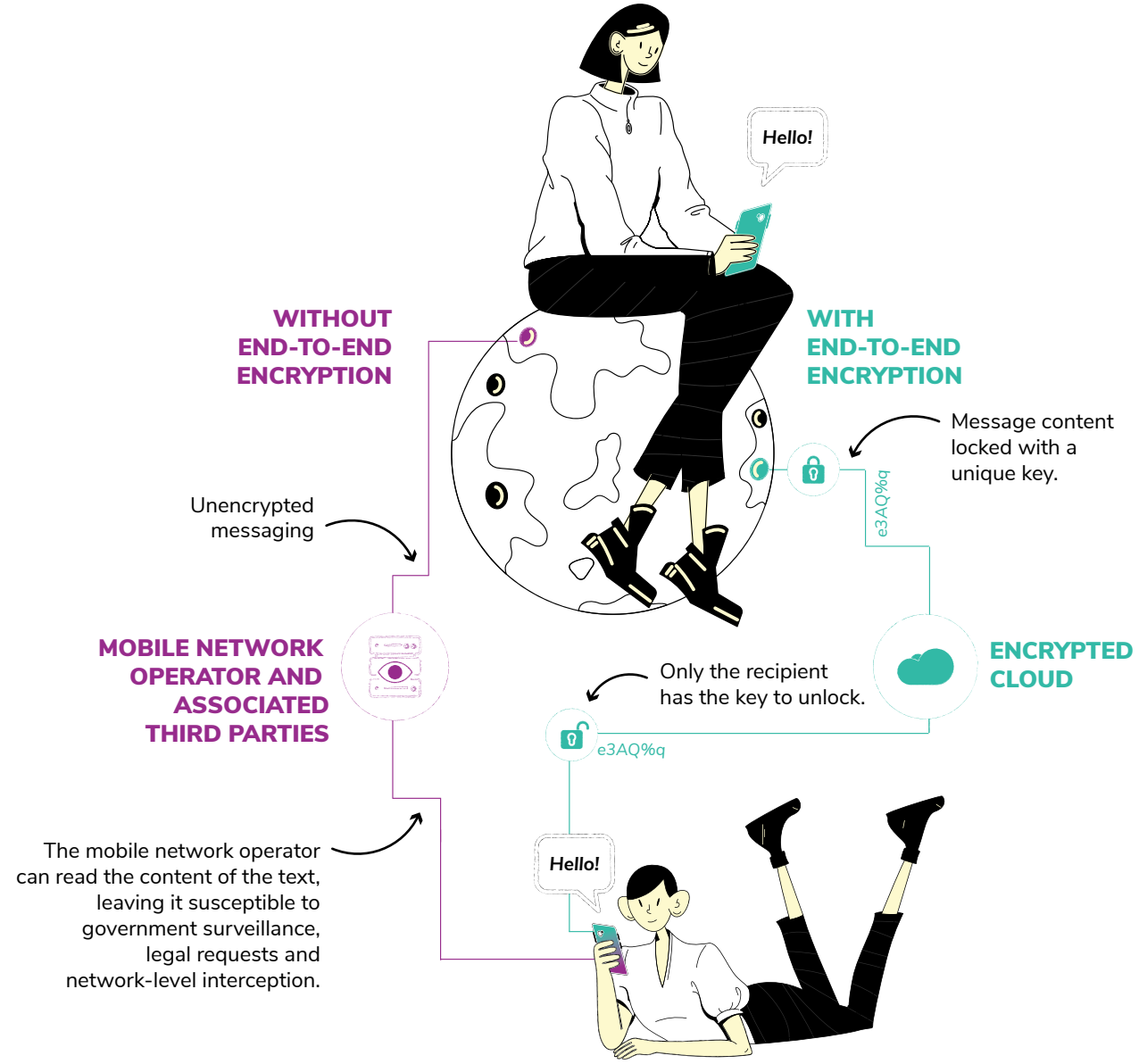
Breaking encryption also benefits state-backed hackers, cybercriminals, foreign adversaries, and other malicious or rogue actors seeking to gain access to government or financial systems.

[74] Satter, R. and Vicens, A.J. (2024). US government tells officials, politicians to ditch regular calls and texts. Reuters.

[75] Politico (2025). European Parliament urges lawmakers to only use encrypted messages after China hacks.

HOW END-TO-END ENCRYPTION KEEPS CONVERSATIONS SECURE

End-to-end encryption ensures that only the sender and intended recipient can read a message. No one else—not the internet provider, not the app, not the government—can access the content.



Indeed, hackers have exploited backdoors in state-of-the-art encrypted platforms to breach highly sensitive US government systems at least twice over the past decade.[76] Law enforcement and security agencies have other more proportionate investigative measures to support their work while still maintaining the immense benefits to people that end-to-end encryption provides, such as targeting the actors using the services for criminal activities, rather than the services themselves. For example, German, French, Spanish and Dutch authorities carried out arrests and raids to halt the operations of Matrix, an invite-only encrypted platform used to facilitate money laundering and arms trafficking.[77]

Blocking and Criminalizing the Use of Encryption Tools

As of March 2025, at least 17 of the 72 countries covered by FOTN 2024 saw blocks on access to services that offer end-to-end encrypted communications, like Signal and ProtonMail, in the past five years.[78] These blocks all occurred in countries ranked Not Free and Partly Free, and were often imposed in response to protests, conflict or unrest—making clear that they are part of a larger toolkit of digital repression.[79] In July 2024, Myanmar's military blocked Signal, cutting people off from one of the most secure communication platforms.[80] Also in 2024, the Russian government blocked Signal and the encrypted messaging application Viber, painting the tools as facilitating terrorist activities.[81]

The blocking of encrypted platforms often coincides with restrictive laws criminalizing their use. In Cuba, encryption has been prohibited except by government approval since at least 2015.[82]

---

76 Reuters (2024). China-linked hackers stole surveillance data from telecom companies, US says; Robertson, J. (2021). Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role. Bloomberg.

77 Antoniuk, D (2024). Police shutter MATRIX encrypted chat service used by criminals. The Record; Politie (2024). Opnieuw versleutelde communicatiedienst criminelen ontmanteld.

78 See Background data.

79 Freedom House (2024). Myanmar.

80 Radio Free Asia (2024). Myanmar junta restricts more mobile apps, residents say.

81 Reuters (2024). Signal messenger blocked in Russia, says Roskomnadzor.; Antoniuk, D. (2024). Russia bans Viber, claiming app facilitates terrorism and drug trafficking. The Record.

82 Cartaya, R. (2015). UN Rapporteur criticizes control of personal data encryption in Cuba. Martinoticias; Permanent Mission of Cuba to the UN (2015). Nota 211/2015.

Cuban authorities have restricted access to end-to-end encrypted platforms during moments of political unrest, such as by blocking Signal during anti-government protests in 2021.[83]

Similarly in Libya, the country's 2022 Anti-Cybercrime Law imposes stringent regulations for encrypted tools. Libyans must obtain a license and approval from the National Information Security and Safety Authority before producing, using or importing encryption technology. Violators face a minimum of 10 years in prison and a fine of up to 150 000 dinars (equivalent to approximately EUR 18 000) in cases where the tools are deployed against the government, banks, the military or security institutions.[84]

The narrative associating these tools with criminal activity has found a foothold among law enforcement agencies in democratic countries, albeit accompanied by less aggressive state action than the blocks and criminalization seen in more authoritarian contexts. In August 2022, Australian authorities barred climate activists arrested for holding an unauthorized protest from using encrypted communication services as a part of their bail conditions.[85] French prosecutors litigating a controversial terrorism case in late 2023 argued the defendants' use of encrypted messaging applications showed they had proof of criminal intent.[86]

Compelled Decryption and Backdoor Pressure

Governments worldwide have passed laws or exerted informal pressure to require that companies provide exceptional access to encrypted content, commonly referred to as a 'backdoor', or decrypt communications at law enforcement request. These measures require companies to fundamentally break their end-to-end encryption standards. This weakening of encryption creates a vulnerability that malicious actors can exploit,[87] undermines the functioning of the global internet and allows authorities to snoop on government critics, independent journalists and activists.

---

83 OONI (2021). How countries attempt to block Signal Private Messenger App around the world.

84 Annir Initiative (2021). The Cybercrime Law – A New Bogeyman to Silence Voices (translated); Human Rights Watch (2023). Libya: Revoke Repressive Anti-Cybercrime Law.

85 Bigle, A. (2022). Blockade Australia climate activist can't use encrypted apps, must let police access phone. ABC.

86 La Quadrature (2023). Criminalization of encryption: the 8 December case; La Quadrature (2023). Encryption discussion during the 8 December trial: from myth to reality.

87 Almeida, D. (2021). A Digital Dystopia: How Calls for Backdoors to Encryption Would Ruin the Internet for Everyone. Internet Society.

Laws mandating backdoors or enabling authorities to compel decryption at request have long been in place in the world's bastions of digital repression, such as Rwanda[88] and Vietnam.[89] In 2020, authorities in Pakistan amended the country's telecommunications regulatory framework to require that social media and communications platforms decrypt messages when mandated by intelligence agencies.[90] In a country where security agencies routinely arrest people for their critical speech, such a requirement raises the risk of repression considerably. For instance, in February 2024, the Pakistani Federal Investigation Agency arrested video blogger Asad Ali Toor for posts he made criticizing judges, the military and the election commission.[91]

Similarly, Russia's 2016 Yarovaya Law requires that online services offering encryption, including end-to-end encrypted messaging services, decrypt content or share encryption keys at the request of intelligence agencies. The law also requires that communications platforms store the content of users' online communications, which is not possible for services that provide end-to-end encryption and do not collect this data. In a February 2024 ruling on these provisions of the Yarovaya Law, the European Court of Human Rights ruled that blanket data retention mandates and compelled decryption orders undermine end-to-end encryption and, as a result, threaten human rights. The court's landmark ruling noted that law enforcement had other investigative measures at their disposal, and concluded that measures that degrade encryption while lacking safeguards 'cannot be regarded as necessary in a democratic society'.[92]

Different approaches to encryption have resulted in debates across Europe. In February 2025, Apple announced that it would no longer offer end-to-end encryption for iCloud users based in the United Kingdom. End-to-end encryption ensures that data stored on the iCloud service can only be decrypted on a person's device, even if Apple's cloud storage is breached by bad actors. Apple's announcement came after the UK government reportedly pressured the company to provide access to any encrypted content on the platform, including for people in other countries, under a sweeping 2016 surveillance law.[93] The UK's backdoor mandate

88 Article 19 and Access Now (2020). Joint submission to the Universal Periodic Review of Rwanda.

89 Secdev Foundation (2016). Vietnamese Cyber Security Law Threatens Privacy Rights and Encryption.

90 Ministry of Information Technology and Telecommunication (2020). Document.

91 Hussain, A. (2024). Pakistani journalist arrested for social posts against government officials. Al Jazeera.

92 European Court of Human Rights (2024). Case of Podchasov v. Russia.

93 Menn, J. (2025). U.K. orders Apple to let it spy on users' encrypted accounts. Washington Post; Page, C. (2025). UK quietly scrubs encryption advice from government websites. TechCrunch.

DIGITAL REPRESSION IN IRAN

Escalation Timeline

2016

MAY

The Supreme Cyberspace Council orders foreign messaging apps to move Iranian users' data to local servers.

2017

APRIL

A judicial order blocks Telegram's newly launched voice-call feature nationwide ahead of the May 2017 elections.

2018

APRIL

Officials permanently ban Telegram after it refuses to relocate data servers to Iran or comply with content regulations. The government launches a state-approved messaging app, Soroush.

2019

NOVEMBER

Authorities impose a near-total internet shutdown for 12 days, leaving only the state-controlled National Information Network accessible and cutting off virtually all outside communications.

2020

MAY

Censorship expands to core internet infrastructure as Iran starts blocking encrypted DNS traffic using deep packet inspection tactics to target secure internet protocols.

2021

JANUARY

Iranian providers remove Signal from local app stores and blocked its service after a surge in users switching from WhatsApp.

JULY

Lawmakers advance a draft 'User Protection Bill' that would force foreign platforms to comply with Iran's rules and criminalize the use of VPNs.

2022

SEPTEMBER

Officials severely restrict connectivity by cutting mobile data in many areas and blocking Instagram and WhatsApp nationwide.

OCTOBER

The ICT Ministry announces that anyone selling or using unlicensed VPNs or other anti-filtering tools can be prosecuted under Article 753 of the penal code.

2024

FEBRUARY

The Supreme Council of Cyberspace issues new regulations banning the use of any VPN or 'refinement-breaking' tool without a government permit.

was widely criticized for undermining privacy and its extraterritorial effects, including by civil society organizations[94] and the US government.[95]

Swedish authorities introduced a proposal in November 2024 that sought to amend the country's legal framework for secret surveillance to mandate that companies with end-to-end encryption services retain communications and decrypt them on receipt of a law enforcement order.[96] Notably, the Swedish Armed Forces criticized the bill and stated that the provision could not be implemented 'without introducing vulnerabilities and backdoors that could be exploited by a third party'.[97]

Across the Atlantic, the debate on encryption has emerged in the patchwork of US state-level technology policy regulation. In Florida, the state Senate passed a bill in April 2025 that compels platforms to decrypt messages from or to the account of a minor when law enforcement obtains a subpoena.[98] The framework incentivizes platforms to remove end-to-end encryption for young people's accounts to facilitate investigations and grant legal guardians the ability to view their messages. Protecting children online is an imperative policy aim. Eroding end-to-end encryption to do so, however, opens new risks for exploitation, for example by leaving the messages and media that children share online less secure and less private.[99]

Civil society, technical experts and some national legislators have played a critical role in addressing problematic proposals that would introduce backdoors, highlighting how diverse actors can leverage democratic processes and independent oversight mechanisms to protect end-to-end encryption. In France, an amendment proposed to a drug-trafficking law would have required encrypted messaging applications and email services to develop technology to allow law enforcement officers to secretly join group chats, known as the 'ghost' model.[100] While

---

94 Amnesty International (2025). UK: Encryption order threatens global privacy rights.

95 Office of the Director of National Intelligence (2025). February 25, 2025 Letter.

96 Regeringen (2025). Utkast till lagrådsremiss; Smalley, S. (2025). Swedish authorities seek backdoor to encrypted messaging apps. The Record.

97 Försvarsmakten (2025). FM2024-28855:2.

98 Florida Senate (2025a). Senate Bill 868 Text; Florida Senate (2025b). Senate Bill 868.

99 Whittaker, Z. (2025). Florida draft law mandating encryption backdoors for social media accounts billed 'dangerous and dumb'. TechCrunch. Klosowski, T. (2025). Florida's New Social Media Bill Says the Quiet Part Out Loud and Demands an Encryption Backdoor. Electronic Frontier Foundation.

100 Internet Society (2020). Fact Sheet: Ghost Proposals.

the amendment passed in the Senate in January 2025 with support from the Interior Ministry, the country's National Assembly in March rejected it after widespread criticism from French and global civil society, the technical community and opposition politicians.[101] Civil society organizations have also raised concerns about the prospect of a 'technological road map' for gaining lawful access to encrypted data proposed in the EU's internal security strategy, which was presented in April 2025.[102]

Traceability Mandates

Building on this desire for greater control online, several governments have sought to compel companies to ensure that they can identify the sender of messages posted or forwarded on their services. Referred to as 'traceability' or 'first-originator' mandates, these measures would force companies to undermine end-to-end encryption. An Internet Society review of technical proposals for implementation found that such requirements entail embedding more information in encrypted messages, fundamentally weakening their integrity, or collecting data or metadata on all users, undermining confidentiality.[103]

Indian authorities have sought to require messaging services to identify the original sender of messages that have been forwarded. The Intermediary Rules 2021 require that companies with at least 5 million domestic users be prepared to identify the original sender of messages in certain cases related to public order, sexually explicit or child abuse material and India's sovereignty, integrity and security. WhatsApp filed a lawsuit challenging the provision on privacy grounds, and a court in Tripura prevented law enforcement from invoking the provision.[104] WhatsApp has stated that it would end service provision in the country if compelled to break end-to-end encryption,[105] which would leave the country's hundreds of millions of WhatsApp users without access to a tool that has become a bedrock for communication, expression and small

[101] Le Monde (2025). L'Assemblée nationale vote pour le maintien de la confidentialité des messageries cryptées, lors d'une nuit agitée; La Quadrature (2025). All-out mobilization against the French 'war-on-drugs' law.

[102] European Commission (2025). COM/2025/148 final.

[103] Internet Society (2024). Traceability in End-to-End Encrypted Environments.

[104] Medianama (2023). Tripura HC Stays Lower Court's Order Asking WhatsApp To Disclose First Originator Of A Message.

[105] Rajan, N. (2021). WhatsApp moves Delhi HC against traceability clause in IT rules, calls it is unconstitutional. The Indian Express; Bhan, I. (2024). WhatsApp tells Delhi High Court it will shut down if forced to break encryption. The Economic Times.

business transactions. In December 2023, Indian lawmakers passed the Telecommunications Act, which includes a requirement for companies to disclose communications in 'an intelligible format', raising concerns that this provision would be used in lieu of the Intermediary Rules' traceability provisions to compel decryption.[106]

A similar proposal stalled in Brazil in the face of widespread criticism from civil society and the private sector.[107] In 2020, the Senate passed a proposal dubbed the 'fake news bill' that would have compelled companies to retain messaging data to ensure the traceability of viral content, defined under the law as those forwarded by more than five users with reach to at least 1 000 accounts, for three months. Subsequent versions of the bill dropped the traceability clause.

Debates Over Client-side Scanning

Several governments have enacted or proposed laws that would compel end-to-end encrypted messaging applications to introduce 'client-side scanning', a technology that 'refers to systems that scan message contents—i.e., text, images, videos, files—for matches or similarities to a database of objectionable content before the message is sent to the intended recipient', according to the Internet Society.[108] Supposedly privacy-protective implementations of the mechanism would deploy hashing, by which a person's device creates a unique digital fingerprint of a piece of content that is then compared to a database of fingerprints of previously known objectionable content. However, technologists and cybersecurity experts have found that client-side scanning is fundamentally incompatible with end-to-end encryption, and can introduce new vulnerabilities that bad actors can exploit.[109]

The UK Online Safety Act, passed in September 2023, could be used to mandate client-side scanning, though lawmakers have delayed the application of the relevant provision until it is 'technically feasible'.[110] The law empowers the communication regulator to mandate that online services employ government-approved software to screen user content for child sexual abuse imagery (CSAM) 'whether communicated publicly or privately by means of the

[106] Freedom House (2024). India.

[107] Freedom House (2022). Brazil.

[108] Internet Society (2020). Fact Sheet: client-side scanning.

[109] Ibid; Abelson, H. et. al. (2021). Bugs in our Pockets: The Risks of Client-Side Scanning. Journal of Cybersecurity.

[110] UK Parliament (2023). Online Safety Bill.

service'.[111] Signal informed UK policymakers that they would make the platform inaccessible in the country if regulators invoked the client-side scanning requirement, raising concerns it would fundamentally undermine the security of their services.[112] Similarly, Australian email provider Fastmail joined Signal, Proton and others in pushing back against an effort by the country's eSafety Commissioner to compel file hosts and email providers to introduce hash-matching for illegal content.[113]

Client-side scanning has also been discussed at the European Union level, including in negotiations over the proposed Regulation on Child Sexual Abuse.[114] The Belgian and Hungarian presidencies of the Council of the European Union advocated for an approach that would require communication platforms, including encrypted services, to implement a form of client-side scanning to detect CSAM for all user-uploaded visual media.[115] Legislators in the European Parliament advanced an alternative approach that would establish safeguards for end-to-end encryption within the framework's text.[116] Amidst the yearslong negotiations over the regulation, Dutch lawmakers in the country's House of Representatives passed two separate measures in 2023 calling on the government to protect encryption and resist client-side scanning at the EU level.[117] Poland, after assuming the EU presidency in January 2025, proposed an approach that would permit platforms to voluntarily implement client-side scanning for CSAM; the Polish proposal affirms that end-to-end encryption should not be weakened.[118]

---

111 Klovig Skelton, S. (2024). Ofcom publishes Illegal Harms Codes of Practice. Computer Weekly; Clark, L. (2024). Now Online Safety Act is law, UK has 'priorities' – but still won't explain 'spy clause'. The Register.

112 Wiggers, K. (2023). Meredith Whittaker reaffirms that Signal would leave UK if forced by privacy bill. TechCrunch.

113 Nadel, J. (2024). eSafety's online storage and message scans 'not technically good' solution says Fastmail. itnews.

114 European Commission (2022). COM/2022/209 final; European Parliament (2024). Briefing on combating child sexual abuse.

115 Meister, A (2024). Belgium wants to oblige users to agree to chat control. Netzpolitik; Council of the European Union (2024). 12406/24.

116 Patrick Breyer (2023). Historic agreement on child sexual abuse proposal (CSAR): European Parliament wants to remove chat control and safeguard secure encryption.

117 Freedom House (2024). Netherlands.

118 EDRi (2025). Poland searches for silver bullet for CSA Regulation; Council of the European Union (2025). 5352/25.

STORIES OF RESISTANCE AND RESILIENCE

Civil society, the private sector and policymakers have driven innovative ways of using and protecting anti-censorship tools and end-to-end encryption.

Despite a ban on Tor since 2015, **Belarusians** have used the service during moments of mass civil engagement, particularly during the pro-democracy movement that mobilized in response to the fraudulent 2020 presidential election.

VPN Generator, a project started by **Russian** dissidents, provides users with distinct, small-scale VPNs servicing 250 users, making it more difficult for authoritarians to block their services.

After the Iranian government blocked access to Signal in 2021, developers added a new feature to the platform that empowered its users to deploy lightweight proxy servers. The service allowed **Iranians** to bypass the block, securely route traffic to the platform and continue communicating safely in a heavily surveilled environment.

Supreme Court jurists in **Brazil** have issued nonbinding opinions to affirm that encryption is essential for fundamental rights and freedoms. In one 2020 intervention, Supreme Court Justice Edson Fachin urged his colleagues to 'recognize that weakening encryption is weakening everyone's right to a secure internet'.

A civil society coalition in **Mauritius** mobilized to prevent the passage of a 2020 bill that would have established an authority to compel the decryption of all internet traffic in order to scan it for 'harmful and illegal contents'.

Chilean policymakers published a cybersecurity framework in April 2024 that affirms that 'every person has the right to adopt the technical computer security techniques that they consider necessary, including encryption'. The framework's language reflects the advocacy of civil society organizations organized under the Alianza por el Cifrado en Latinoamérica y el Caribe (Alliance for Encryption in Latin America and the Caribbean).

05

Policy Recommendations

Safeguarding access to anti-censorship and end-to-end encrypted tools is fundamental to protecting the free and open internet, strengthening national security and advancing economic growth and innovation. Despite the rising restrictions on these tools that this report identifies, those committed to a free and open internet will continue to innovate to ensure that these services meet the moment and can help create an internet where privacy and open access are the default. Technologists and developers, for example, are building more secure and resilient tools, such as integrating anti-censorship technology into widely used web protocols. Civil society organizations are working closely with democratic policymakers to pass laws that protect end-to-end encryption and affirm its importance for fundamental freedoms.

The following recommendations lay out strategies that policymakers, regulators, donor institutions and private companies can adopt to protect access to anti-censorship tools and end-to-end encryption, and safeguard the free and open internet more broadly.

Recommendations for Governments

1. Protect access to anti-censorship tools

Governments should refrain from blocking, criminalizing or imposing restrictions on access to anti-censorship tools and respect the international human rights principles of necessity, proportionality and legality when considering any such decisions. As part of this, policymakers should consult the private sector, civil society organizations and the technical community to assess the implications of such measures they are considering imposing. Authorities should avoid laws that mandate onerous registration, data retention or content restriction requirements, which can undermine the privacy, security and anti-censorship benefits the tools provide and could compel providers to exit the country or terminate their services.

2. Safeguard end-to-end encryption

Governments should refrain from blocking, criminalizing or imposing restrictions on access to end-to-end encryption tools. To avoid weakening the technology, governments should not pass laws that introduce mandates for backdoors, traceability, client-side scanning or restrictions on cryptography that compromise secure communication. Legal and regulatory frameworks

should affirm that providing strong end-to-encrypted services is lawful, protected and essential for safeguarding human rights, cybersecurity, national security and financial systems.

Laws that regulate social media and communications platforms, including content regulations that have takedown requirements and reforms to intermediary liability standards, should explicitly carve out end-to-end encrypted services. Without such exceptions, companies would need to break encryption for compliance, undermining the essential protections that cryptography provides.

3. Invest in proven and rights-based responses to crime

Governments have a responsibility to protect their populations from terrorism, violence, child sexual abuse and other heinous crimes that use the internet in their facilitation. Policymakers should invest in mechanisms that mitigate these challenges in a way that aligns with international human rights standards of necessity, proportionality and legitimacy, rather than pursuing responses that break end-to-end encryption or undermine access to anti-censorship tools. For example, law enforcement can leverage more targeted and narrow surveillance tactics, such as seizing electronic devices and requesting user data in criminal cases. These efforts should be subject to strong due process standards and independent, judicial oversight, including through accessing a legitimate warrant.

As a starting point to prevent, investigate and mitigate online child exploitation and CSAM, governments should ensure that law enforcement agencies have the sufficient resources to respond, including through undercover investigations and other investigative measures subject to judicial oversight. Platform regulation focused on child safety should prioritize protecting children's privacy, including through strong data protection obligations and more stringent safeguards for children's profiles, like restricting unsolicited messages.

Ultimately, policymakers should pursue a whole-of-society approach that incorporates both technical and non-technical solutions to preventing crimes carried out online, such as digital security and online safety education. In doing so, they should work closely with civil society, technical experts, the private sector and survivors of exploitation and violence, all of whom have insights that will help make responses more effective and innovative. For example, the private sector has the technical expertise to help tailor user reporting tools for CSAM, terrorist content or other cybercrimes to function within end-to-end encrypted platforms.

4. Fund programming to defend and extend access to anti-censorship and end-to-end encryption tools

Foreign assistance programming is vital for the development and distribution of cutting-edge anti-censorship and end-to-end encrypted tools. Governments should incorporate this programming into their democracy-assistance strategies, prioritizing support for tools that are privacy-preserving, incorporate best-in-class security standards, and are open-source. Support can also help increase the accessibility of anti-censorship and end-to-end encrypted tools to various communities, such as through translating them into diverse languages, supplying them directly to program beneficiaries, and providing digital-hygiene training.

5. Engage internationally to protect access to anti-censorship and end-to-end encryption

Governments should include the protection of anti-censorship tools and end-to-end encryption in their cyber and digital diplomacy strategies. They should champion anti-censorship and end-to-end encrypted tools within existing global processes like the United Nations' GDC, the DFI and the WSIS+20 Review Process. Governments should also facilitate dialogue about the security, economic and human rights benefits of anti-censorship and end-to-end encryption tools and push back against disproportionate government restrictions within bilateral engagements and other existing bodies (e.g., the Freedom Online Coalition), and, as necessary, through the creation of new coalitions.

6. Promote and strengthen multi-stakeholder model of internet governance

Robust engagement with the private sector, civil society, academia and the technical community is critical for those governments that wish to understand and adequately respond to trends in anti-censorship and encryption developments. Governments should invest in strengthening engagement with these actors, particularly civil society organizations and advocates in countries where use of these technologies is essential for bypassing digital repression. This includes working with bodies and venues that already have a multi-stakeholder structure, such as the Freedom Online Coalition, the Internet Governance Forum (IGF) and IGF regional iterations.

Recommendations for the Private Sector

7. Adopt best practices for privacy, data security, usability and accessibility

Providers of anti-censorship tools and end-to-end encrypted messaging services should protect the privacy of their users in design. Providers should create privacy-preserving products that are end-to-end encrypted by default, support anonymity software and collect minimal data. Strong data-minimization practices help companies resist overbroad data requests from governments, providing insulation against demands that carry negative downstream implications for people's rights. Providers should publish regular, independently conducted audits and security assessments to bolster confidence that their products are safe from backdoors or vulnerabilities.

Messaging services, including end-to-end encrypted platforms, should design their products with resilience to censorship in mind. For example, messaging applications can implement domain-fronting or proxy settings to increase the likelihood that they will remain accessible when governments attempt to block them. Such measures can help ensure that people have access to trusted and reliable internet connectivity in crisis situations.

Companies providing services across the internet infrastructure ecosystem should embed anti-censorship functions into their products, which will help cultivate resilience to censorship and surveillance as a default. Intermediaries—including browsers, software companies and Content Delivery Networks (CDNs)—should incorporate anti-censorship tools and capabilities into their offerings or services. CDNs should also strive towards making traffic using an encrypted tunnel indistinguishable from normal traffic, providing users with another avenue to circumvent restrictions.

Affordability is also a major hurdle to anti-censorship technology adoption. Major cloud providers and other intermediaries can reduce this barrier by providing bandwidth credits or discounted rates for VPNs, especially for populations facing political or social crises or other circumstances that make escalated censorship likely. This will help make anti-censorship tools more accessible to those who need them urgently.

8. Adapt tools to the contexts where they are most needed

Providers of anti-censorship tools and end-to-end encrypted services should ensure their products meet the various needs of their users and respond to the diverse contexts in which governments impose censorship and surveillance. Continuous dialogue with local civil society organizations, particularly those focusing on the experiences of communities and users who are vulnerable to harm and repression, offers a pathway to facilitate such assessments. This could mean co-developing circumvention toolkits for at-risk communities or supporting the translation of secure communications apps. Tools should be tested in the local context prior to wider rollout and be adapted based on evolving conflict analyses to mitigate risk. Product changes may include adjusting VPN server configurations to evade new blocking techniques or optimizing apps to use less bandwidth.

This cross-sector learning and collaboration will enhance local confidence in anti-censorship and end-to-end encryption technologies, and ideally thereby increase adoption of these tools. In this way, companies can help maximize the ability of their tools to protect people from government repression.

9. Uphold human rights commitments when facing government demands

Providers of anti-censorship and end-to-end encrypted platforms should resist government requests for user data or content restrictions that contravene international human rights standards. Operators of app stores should also resist government demands to remove anti-censorship tools and end-to-end encrypted messaging applications. In doing so, companies should use all available legal channels to challenge such problematic requests from state agencies, whether they are official or informal. This includes bringing strategic legal cases that challenge government overreach, in consultation or partnership with civil society. Companies should also thoroughly document government demands internally, notify impacted users as to why content may be restricted or data was handed over and publish transparency reports of government demands.

10. Support civil society resilience to defend anti-censorship tools and end-to-end encryption

Companies should collaborate with civil society on joint and sustained efforts to defend access to anti-censorship and end-to-end encrypted tools, and the free and open internet more broadly. This could include joining advocacy coalitions against restrictions on end-to-end encrypted services or supporting timely litigation to challenge laws that undermine the accessibility of anti-censorship tools. Companies should also provide direct support to civil society organizations for this work, and provide in-kind support for resources such as free licenses to use anti-censorship tools.

06

Glossary of Terms

Anti-censorship tools: Digital tools designed to bypass online censorship, allowing users access to blocked content; some may also protect online privacy by encrypting internet traffic or masking the identities of users. They are also commonly referred to as 'circumvention tools.'

Content delivery network (CDN): A globally distributed network of servers that stores copies of web content closer to end users, enabling faster and more reliable access to websites and services around the world.

Cryptographic backdoor (or 'encryption backdoor'): A deliberate vulnerability built into secure systems that allows those who know of it to significantly reduce the security of the system or bypass it entirely.

Deep packet inspection (DPI): A technique used to examine or analyse the content of internet packets transmitted over a network, often employed by governments to monitor, filter or block internet traffic.

Domain Name System (DNS) resolver: The Domain Name System translates names that are meaningful to humans (web addresses) into data used by computers (numerical IP addresses) so that internet users can visit websites. DNS resolvers are servers that facilitate the conversion.

Domain fronting: A method used by some anti-censorship tools to disguise internet traffic by routing requests through permitted domains, making it difficult for censors to identify and block them.

Encryption: A method of scrambling and unscrambling data through a cryptographic algorithm to protect against unauthorized access. The process is usually facilitated by encryption keys, pieces of information used to scramble and unscramble data.

End-to-end encryption (E2EE): A system of encryption whereby only the sender and intended receiver of a message (or other forms of data) have the necessary encryption keys. It is designed to prevent third parties, including the operator of the messaging service and telecommunications providers, from accessing encrypted content, and is widely considered the strongest form of encryption.

Internet Protocol (IP): A set of rules governing the formats and methods for transmitting data sent over the internet, including unique numerical addresses (IP addresses) assigned to devices connected to a network.

Proxy connection: A method of connecting to the internet through an intermediary server that forwards requests and responses between a user and the websites they access.

Quick UDP Internet Connections (QUIC): A network protocol designed to improve the performance and security of web traffic, combining speed advantages of older protocols with better security and encryption.

Transport Layer Security (TLS): A widely used encryption protocol designed to secure data sent between applications over the internet. TLS helps avoid the possible surveillance or alteration of transmitted data, forming the backbone of secure internet services such as HTTPS.

Virtual private network (VPN): A digital service that encrypts and routes internet traffic through an external server, masking a user's real location and protecting their data from surveillance and censorship.

07

About the Report and Methodology

This report was produced as part of the Global Initiative on the Future of the Internet (GIFI), led by the European University Institute. GIFI is an EU-funded project established to promote the Open Internet and the principles and commitments of the DFI, and support the implementation of DFI principles through a collaborative and rights-based approach. The views expressed in this report are an independent analysis and do not represent the official position of the European Union or any of its institutions, bodies and agencies.

This report builds on the work on digital authoritarianism undertaken by the European University Institute and expands on the evidence of these practices gathered by Freedom House over the past 15 years. The report used a mixed-methods research approach that combined desk research and interviews with technical, policy, product and country-specific experts, including during a closed-door workshop in February 2025. It focused on developments that occurred between January 2020 and May 2025. It analysed trends in countries and regions around the world, with a particular focus on the 72 countries included in Freedom House's *Freedom on the Net 2024* report.

08

Acknowledgements

The authors are grateful to Nayia Barmpaliou, Gerardo Berthin, Annie Boyajian, Jennifer Brody, Cathryn Grothe, Stephanie Hoffman and Adrian Shahbaz for their valuable feedback on the report. Aashna Agarwal, Matthew Barak, Mina Loldj, Maddie Masinsin and Elizabeth Sutterlin were also instrumental to the research process.

The European University Institute and Freedom House also extend their gratitude to the external individuals whose expertise informed the report. Those that provided feedback on the draft report include:

» Alena Epifanova, research fellow for digital policy and democracy, German Council on Foreign Relations
» Ksenia Ermoshina, researcher at the Center for Internet and Society (CNRS) and The Citizen Lab; lead researcher, eQualitie
» Arturo Filastò, executive director and chief technology officer, the Open Observatory of Network Interference (OONI)
» Apar Gupta, advocate and founder director, Internet Freedom Foundation
» Irene Poetranto, independent researcher
» Ryan Polk, director of internet policy, Internet Society
» Amir Rashidi, director of digital security and rights, Miaan Group

The multi-stakeholder group of experts who attended a workshop on threats to anti-censorship and encryption tools include: Aljosa Ajanovic Andelic, Christine Bannan, Jon Camfield, Patricija Cerniauskaite, J. Alex Dalessio, Robyn Greene, Samvel Martirosyan, Al Smith, Dr. Quoc-Hung Tran and Callum Voge.

09

About the Authors

Grant Baker is a research analyst for technology and democracy at Freedom House. He covers Europe and Eurasia for *Freedom on the Net*. Prior to joining Freedom House, he worked as the Research Manager at SMEX, where he led the Beirut-based organization's research on digital rights from 2018 to 2020. In 2016, he interned at Harvard University's Berkman Klein Center for Internet and Society, providing research assistance on their freedom of expression projects. Baker graduated cum laude from Amherst College with a degree in Asian Languages and Civilizations (focusing on the Middle East) and studied Arabic.

Nils Berglund is a research associate at the Robert Schuman Centre for Advanced Studies, and project lead for GIFI. His expertise centers around the European Union's cyber and digital diplomacy, the global governance of the internet and sustainable digital transformation. Through GIFI and other projects, he works with governments, international organizations and the broader multi-stakeholder community to provide policy support, outreach and capacity-building on cyber and digital issues. Before joining the EUI, Berglund worked at the EU Institute for Security Studies, where he was the project coordinator of the EU Cyber Diplomacy Initiative–EU Cyber Direct. He has previously served as a research fellow at Research ICT Africa, and managing editor for the Directions Blog. He holds a Master of Science in Media and Communications from the London School of Economics and Political Science.

Allie Funk leads Freedom House's technology and democracy initiative, including *Freedom on the Net*. She also represents Freedom House on the Freedom Online Coalition's Advisory Network, serves on the Global Network Initiative's Board of Directors, and is a Council on Foreign Relations term member. Her writing has been published in the *Washington Post*, the *Los Angeles Times*, *WIRED*, Lawfare, the Hill, the Diplomat and Just Security, among others. Prior to joining Freedom House, Funk worked at the National Association of Criminal Defense Lawyers on issues relating to reforming US surveillance practices, closing the Guantanamo Bay detention facility and protecting the right to counsel, and also worked with Human Rights First's foreign policy team. She holds a master's degree in human rights from the London School of Economics and Political Science and a BA in philosophy and political science from the University of Louisville.

Patryk Pawlak is a part-time professor at the Robert Schuman Centre and project director for GIFI. His fields of expertise are global governance of digital and cyber issues, the impact of technology on foreign and security policy and the European Union's cyber and digital diplomacy. Patryk advises and consults for governments, international organizations and various

EU initiatives on cyber and digital diplomacy. He has been involved in multilateral cyber-related processes at the United Nations and bilateral consultations between the EU and partners. Prior to joining EUI, Pawlak headed the Brussels office of the EU Institute for Security Studies (EUISS) and coordinated the institute's cyber and digital activities. From 2018 to 2022, he was project director of the EU Cyber Diplomacy Initiative–EU Cyber Direct. In this capacity, he ideated and coordinated numerous initiatives, including EU Cyber Consultations with partner countries, the European Cyber Diplomacy Dialogue and the EU Cyber Forum. Pawlak is also a visiting scholar at Carnegie Europe. He holds a PhD in Social and Political Sciences from the European University Institute.

Kian Vesteinsson is senior research analyst for technology and democracy at Freedom House. He manages research and writes for *Freedom on the Net*, and previously covered Asia and sub-Saharan Africa for the publication. Before joining Freedom House, Vesteinsson was senior law and tech policy officer at Human Rights Watch, where he staffed the office of the general counsel and contributed to research and advocacy on human rights and technology around the world, focusing on surveillance in the United States. Previously, he worked on digital privacy, police technology and national security surveillance at the National Association of Criminal Defense Lawyers. Vesteinsson holds a BA in Politics and Religious Studies from Pomona College.

EUROPEAN UNIVERSITY INSTITUTE

Published by

European University Institute (EUI)

Via dei Roccettini 9, I-50014

San Domenico di Fiesole (FI)

Italy

www.eui.eu

ISBN:978-92-9466-674-1
doi:10.2870/8871367
QM-01-25-099-EN-N

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union.