



INTERNET
INFRASTRUCTURE
COALITION

VPNs at Risk: An “Internet at Risk” Report

Understanding Virtual Private Networks,
Their Role in Cybersecurity, and Global
Case Studies on Regulating Their Use



Table of Contents

2026

Executive Summary	2
Part I: Understanding VPN Technology	3
1. What Is a VPN?	3
2. How VPNs Actually Work	6
Part II: What Users Should Know	10
3. Understanding Privacy	10
4. Information Collection, Logs, and Data Retention	13
5. Jurisdiction Matters	16
6. Choosing a VPN	18
Part III: The Role of VPNs in a Secure Internet	20
7. Protecting People, Not Just Networks	20
8. VPNs as Critical Cybersecurity Infrastructure	23
9. VPN Critics and Infrastructure Neutrality	25
Part IV: VPNs Under Pressure	27
10. Why Governments Are Regulating VPNs	27
11. Case Studies	29
Part V: Looking Forward	36
12. Policy Considerations for a Secure Internet	36
13. Conclusion	39



Executive Summary

Virtual private networks, or VPNs, are among the most widely used and widely misunderstood security technologies on the Internet. They are often described as consumer privacy tools, applications for remote workers, or technologies that allow users to access services from another location. Each description captures part of their use, but none fully explains their role.

At their core, VPNs are secure networking technologies. They create encrypted connections across untrusted networks, allowing individuals and organizations to communicate more securely over the public Internet. Long before consumer VPN services became widely available, VPNs were used to connect employees, offices, data centers, and protected systems at businesses, governments, universities, and other institutions. Today, the same underlying capabilities support enterprise cybersecurity and infrastructure, while also helping ordinary Internet users protect their communications as they work, travel, bank, shop, and connect across networks they do not control.

Understanding that broader role is increasingly important as governments consider measures affecting VPN providers and VPN use. This report explains how VPN technology works, the security and privacy functions it provides, and the responsibilities of providers, and examines through international case studies the different ways governments have approached VPN regulation.

Those case studies demonstrate an important distinction: regulating the business practices of a commercial VPN provider is not the same as blocking VPN protocols or imposing requirements on the infrastructure supporting them. VPN regulation can include data-retention requirements, provider licensing, blocking obligations, penalties for circumvention, restrictions on distribution, and network-level interference. These measures operate at different technical layers and can produce different consequences.

Governments have legitimate policy objectives involving cybersecurity, national security, criminal investigations, child protection, public safety, copyright enforcement, and access to online content. As with other technologies, some capabilities provided by VPNs can complicate network attribution, allow users to circumvent restrictions, or make particular enforcement mechanisms less effective. At the same time, those features also support secure remote work, corporate networks, journalism, research, personal safety, and ordinary Internet use. VPNs are general-purpose technologies used by businesses, institutions, governments, and individuals. Their technical capabilities do not determine the intent of the people using them.

The policy question is therefore not simply whether VPNs should be regulated, but how particular harms can be addressed at the appropriate technical layer and by actors positioned to address them. The closer regulation moves toward shared protocols and underlying Internet infrastructure, the greater the need to consider potential effects on unrelated lawful users and services. An intermediary is a service provider that carries, hosts, routes, or otherwise enables another party's online activity. Restrictions can target VPN providers, underlying network infrastructure, or distribution channels. In particular, requirements imposed on cloud providers, data centers, Internet service providers, or other intermediaries can extend responsibility to actors far removed from—or wholly uninvolved in—the conduct policymakers seek to address.

Effective VPN policymaking therefore requires precision. Policymakers should clearly identify the harm they seek to address, determine which actors have meaningful knowledge of and control over that harm, and consider whether regulation is directed at the appropriate technical layer. They should also evaluate potential consequences for cybersecurity, privacy, critical infrastructure, lawful users, and the resilience and openness of the Internet.

Precision does not mean that VPN providers or other Internet intermediaries should operate without responsibility. Industry should strengthen trust through secure engineering, data minimization, clear privacy practices, independent audits, transparency reporting, effective, responsible governance, and meaningful cooperation with legitimate legal processes.

Policymakers do not have to choose between addressing legitimate harms and preserving the security of the Internet. Understanding how VPNs function, distinguishing among the different technical layers at which regulation can operate, and imposing requirements on the actors actually positioned to address the underlying harm can help produce more effective policy and avoid unintended consequences, while preserving the security, interoperability, resilience, and openness of the global Internet.

Part I: Understanding VPN Technology

1. What Is a VPN?

Virtual private networks, commonly known as VPNs, have become one of the most widely discussed technologies operating in the global Internet ecosystem. VPNs are tools recommended by experts¹ as best practices for cybersecurity, used by businesses and citizens around the world, and increasingly scrutinized by governments seeking to regulate online activity. Yet despite their prominence, VPNs remain one of the most misunderstood pieces of Internet infrastructure.

¹National Institute of Standards and Technology (NIST), Murugiah Souppaya & Karen Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, NIST SP 800-46 Rev. 2 (July 2016), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>.

To some, a VPN is simply an app that changes your apparent location online. Others think of it as a tool for anonymity or for accessing content that might otherwise be unavailable. Businesses and governmental bodies, including legislatures, view VPNs as indispensable components of their cybersecurity programs, while policymakers often encounter them in discussions about criminal investigations, online safety, privacy, and censorship. Each of these perspectives contains an element of truth, but none fully explains what a VPN actually is.

This report focuses on VPN technologies that use encryption to protect communications across untrusted networks. At its core, a VPN is neither a product nor a platform. It is a networking technology developed to solve a practical engineering problem: how to securely connect computers across networks that cannot be trusted.² Highlighting and understanding that original purpose is essential because much of today's debate focuses on how VPNs can be used rather than why they were created in the first place.

The Internet Was Never Designed to Be Private

The Internet was built to connect networks, not to guarantee privacy. Its early architects were primarily concerned with allowing computers and independent networks to communicate reliably with one another across different kinds of network infrastructure.³ Security and resilience were certainly considered, but the Internet as a whole—a network of networks⁴—was never intended to function as a private communications system.

As the Internet grew beyond research institutions and government networks into the massive global network we know today, entirely new challenges emerged: businesses transmitting financial information across public networks, employees needing secure access while traveling, hospitals exchanging patient data, and ordinary users banking and shopping online.

In each case, organizations and individuals faced the same fundamental dilemma: how do you safely send sensitive information across infrastructure that you neither own nor control?

VPNs emerged as one answer to that question.

The Problem VPNs Were Designed to Solve

Imagine a company with a single office. Every employee works inside the building, connected to the same internal network that is protected behind a firewall and inaccessible to the outside world. Within that environment, employees can securely access internal

² NIST, Virtual Private Network (VPN), Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/virtual_private_network; B. Gleeson et al., *A Framework for IP Based Virtual Private Networks*, RFC 2764 (2000), <https://www.rfc-editor.org/rfc/rfc2764>.

³ Barry M. Leiner et al., *A Brief History of the Internet*, Internet Society (1997), <https://www.internetsociety.org/internet/history-internet/brief-history-internet/>.

⁴ Internet Society, *The Internet Way of Networking: Defining the Critical Properties of the Internet*, "Decentralized Management and a Single Distributed Routing System" (2020), <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>.

databases, financial systems, and proprietary applications.

Now imagine one employee begins working from a remote client site or from home.

That employee still needs access to many of those same systems, but reaching a private corporate network across the public Internet introduces new risks. The company needs a way to authenticate the employee and protect communications as they travel across infrastructure the company does not control.

A VPN solves this problem by creating a secure, encrypted connection for that remote employee across the public Internet.⁵ Rather than exposing that employee's internal communications directly to outside networks, the VPN establishes what is often described as a "private tunnel" through otherwise public infrastructure that the internal communications can travel through safely. Although the data still traverses the Internet, it does so in a form that is protected from unauthorized observation while in transit.

Importantly, the Internet itself has not become private. Instead, the VPN creates a protected pathway through it. That distinction lies at the heart of how VPN technology works.

VPNs Solved an Enterprise Problem First

One of the most common misconceptions about VPNs is that they began as consumer privacy products. In reality, VPN services for consumer use are a relatively recent development.⁶

Organizations used VPNs to protect their networks before consumer VPN services became widespread.⁷ Key technologies underlying modern VPNs were being standardized by the mid-1990s.⁸ Banks connected branches across wide geographic areas. Manufacturers securely linked factories to corporate headquarters. Universities allowed faculty to access research resources remotely. Governments connected agencies separated by hundreds or even thousands of miles. As remote work expanded, businesses and governments increasingly relied on VPNs to allow employees to securely access internal systems from home, hotels, airports, and customer sites.

Today, enterprise VPNs remain a widely deployed component of organizational cybersecurity, providing employees and other authorized users with secure remote access to protected resources.⁹ Consumer VPN services helped bring VPNs to a wider public audience; they did not invent the technology. They adapted an established enterprise

⁵ NIST, *Guide to IPsec VPNs*, NIST SP 800-77 Rev. 1, § 2.3 (2020), <https://doi.org/10.6028/NIST.SP.800-77r1>.

⁶ Desire Athow, *VPN's Coming-of-Age: A Discussion with the ExpressVPN Co-Founders*, TechRadar (2020), <https://www.techradar.com/news/vpns-coming-of-age-a-discussion-with-the-expressvpn-co-founders>.

⁷ Joel Khalili, *VPNs Have Been Around for Decades, but Have Never Been More Relevant*, TechRadar (2021), <https://www.techradar.com/news/vpns-have-been-around-for-decades-but-have-never-been-more-relevant>.

⁸ R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 1825 (1995), <https://www.rfc-editor.org/rfc/rfc1825.html>.

⁹ NIST, *Mobile Device Security: Bring Your Own Device (BYOD)*, NIST SP 1800-22B (Sept. 2023), <https://www.nccoe.nist.gov/publication/1800-22/VolB/index.html>.

security technology to meet the needs of individual Internet users.¹⁰

This important distinction reframes many of today's policy discussions. Restrictions aimed at consumer VPN services concern more than applications developed for individual privacy. They can also affect the same underlying technology that businesses, governments, universities, healthcare providers, and countless other organizations have used for decades and depend upon every day to secure their own communications.

From Enterprise Security to Internet Infrastructure

As Internet use evolved, so did the role of VPNs. Public Wi-Fi became commonplace, cloud computing moved applications beyond traditional corporate networks, and individuals became more concerned about online privacy and security. Consumer VPN services made an established security capability broadly accessible to individual Internet users.

Today, VPNs support remote work, connect distributed infrastructure, protect communications across untrusted networks, and provide individuals with an additional layer of privacy and security. Journalists, researchers, human rights defenders, and others operating in sensitive environments also rely on them to reduce exposure to surveillance or interference.¹¹

VPNs have become an integral part of the Internet's broader security architecture. The next chapter explains how that infrastructure works, step by step, when a VPN connection is established.

2. How VPNs Actually Work

To understand how a virtual private network protects information, it helps to begin by looking at what happens when someone uses the Internet without one.

Every time a person opens a website, checks email, streams a video, or launches an application, their device begins a conversation with another computer somewhere else on the Internet. Although users often think of the Internet as a single network, it is more accurately a network of networks. Communications may travel across infrastructure operated by Internet service providers (ISPs), backbone and transit providers, Internet exchange points, cloud providers, and hosting companies before reaching their destination.

Understanding that journey is the key to understanding where VPNs fit.

¹⁰ Athow, *supra* note 6.

¹¹ CPJ Emergencies Response Team, *CPJ Launches Digital Safety Kit*, Committee to Protect Journalists (July 30, 2019), <https://cpj.org/2019/07/cpj-launches-digital-safety-kit/>.

Internet Communications Without a VPN

Imagine typing **www.example.com** into your browser.

The first thing your computer must determine is where that website actually lives. Computers do not communicate using domain names; they communicate using Internet Protocol (IP) addresses. Your device therefore sends a request to the Domain Name System (DNS), often described as the Internet's address book, asking which IP address corresponds to the domain you entered.

Once the correct IP address has been returned, your computer begins establishing a connection to that server. Data is transmitted in small units called packets. Each packet contains both the information being transmitted and instructions describing where it should be delivered.

Those packets travel first through your local network and ISP and then through interconnected networks until they reach the infrastructure hosting the destination website or application. Depending on the route, several independent network operators, including ISPs and other operators along the traffic's path, may participate in delivering the communication, each occupying a different position from which it may observe certain aspects of the traffic.

A VPN does not eliminate this journey. Instead, it changes the path the traffic follows and changes who is able to observe it along the way.

Building a Secure Tunnel

When a VPN connection is established, the user's device first authenticates with a VPN server operated by the chosen VPN provider. Before application traffic is carried through the tunnel, the two systems negotiate a secure encrypted session using cryptographic keys that are unique to that connection.



Once the session has been established, traffic routed through the VPN is encrypted before it enters the public Internet. Rather than being sent directly toward its final destination, that traffic is encapsulated inside packets addressed to the VPN server itself.

This process is what engineers refer to as tunneling.

The word "tunnel" can be misleading because no new physical pathway is created. The packets still travel across the same public Internet infrastructure as before. What changes is that traffic routed through the VPN is carried inside an encrypted connection between the user's device and the VPN server, much like sending a sealed letter inside a courier package. Postal workers still move the package, but they cannot read the letter sealed inside. Likewise, Internet infrastructure continues routing VPN traffic normally, while the encrypted contents remain unintelligible to anyone who cannot decrypt them.

When the encrypted packets reach the VPN server, the outer layer of encryption is removed and the server forwards the original request toward its intended destination using its own Internet connection. When the destination responds, the process happens in reverse: the VPN server encrypts the returning packets and sends them back through the secure tunnel to the user's device, where they are decrypted and presented to the application.

From the user's perspective, the entire process is effectively invisible. Web pages load normally and applications behave as expected.

The same basic mechanics can support very different VPN deployments. The endpoint may be operated by an employer, a cloud provider, or a consumer VPN service. What differs is who operates that endpoint, where the traffic goes next, and the trust relationship between the user and operator. Chapter 8 examines those different deployment models in greater detail.

VPN Protocols

Not all VPNs establish secure tunnels in exactly the same way. The rules governing how devices authenticate, encrypt information, exchange keys, and transmit data are defined by protocols.

Several protocols have become widely adopted over the years, each reflecting different engineering priorities.

OpenVPN is an open-source VPN implementation that supports flexible authentication and deployment configurations and has undergone independent security assessments.¹² It supports multiple operating systems and can be used for remote-access and site-to-site connections.

WireGuard is a newer protocol designed with simplicity and performance in mind. Its smaller code base makes it easier to audit, while modern cryptographic techniques often allow it to deliver faster connection speeds with lower overhead.¹³ For example, Mullvad announced a move from OpenVPN to WireGuard.¹⁴

IPsec, often paired with Internet Key Exchange (IKEv2),¹⁵ can be used in enterprise environments to connect offices, data centers, and remote employees, integrating with network infrastructure and operating systems.

¹² OpenVPN, *OpenVPN 2.x Community How-To: Complete Setup & Configuration Guide*, <https://openvpn.net/community-docs/how-to.html>; Jean-Baptiste Bédune, Jordan Bouyat & Gabriel Campana, *Security Assessment of OpenVPN*, Quarkslab (May 11, 2017) (assessing OpenVPN 2.4.0), <https://blog.quarkslab.com/security-assessment-of-openvpn.html>.

¹³ Jason A. Donenfeld, *WireGuard: Next Generation Kernel Network Tunnel*, Network and Distributed System Security Symposium (NDSS) (2017), <https://www.wireguard.com/papers/wireguard.pdf>.

¹⁴ Mark Gill, *Mullvad Is Set to Remove Support for OpenVPN in Six Months – Here's Why*, TechRadar (2025), <https://www.techradar.com/vpn/vpn-privacy-security/mullvad-is-set-to-remove-support-for-openvpn-in-six-months-heres-why>.

¹⁵ C. Kaufman et al., *Internet Key Exchange Protocol Version 2 (IKEv2)*, RFC 7296 (2014), <https://www.rfc-editor.org/rfc/rfc7296>.

No protocol is universally “best.” Organizations choose among them based on security requirements, compatibility, performance, ease of deployment, and the environments in which they operate. All pursue the same objective: establishing an authenticated, encrypted pathway across an otherwise untrusted network.

VPN Servers and Global Infrastructure

A VPN service is much more than an application installed on a user’s device. Many consumer VPN providers operate distributed networks of servers located in data centers around the world, often in the same commercial facilities that host websites, cloud platforms, financial services, enterprise software, and other Internet services. Some VPN providers operate their own physical hardware, while others lease dedicated servers or deploy virtual infrastructure through established cloud providers. The specific approach varies, but the underlying purpose is the same: to place secure points of presence in locations where users can connect reliably.

Individual VPN servers are commonly referred to as **nodes** or **exit nodes**, representing the point where encrypted traffic leaves the VPN network and re-enters the public Internet on its way to the final destination.

Building these networks requires considerable operational planning. VPN providers must distribute servers geographically to reduce latency, maintain sufficient capacity to handle demand, establish redundant infrastructure to improve reliability, and connect their networks to multiple Internet carriers to avoid single points of failure. VPN providers must continually manage capacity, performance, security, resilience, abuse, and availability.

VPN providers form part of the broader Internet security ecosystem, but their functions and technical capabilities differ from those of Internet access providers and other network operators. Those differences matter when assessing appropriate regulatory obligations.

After Traffic Leaves the VPN

One of the most common misconceptions about VPNs is that they somehow remove users from the Internet or make them impossible to identify. Neither is true.

Once traffic leaves the VPN server, it continues across interconnected networks toward its destination. The destination website still receives a request. The response still travels back across interconnected networks. The difference is simply that the destination sees the VPN server as the apparent source of the connection rather than the user’s own residential or enterprise Internet connection.

A VPN changes what different parties can observe, but it does not eliminate the visibility of every participant in the communication. Understanding exactly what information remains visible, and to whom, is an important part of evaluating any VPN service. These distinctions become particularly important when discussing privacy and information collection and retention, the subjects of Chapters 3 and 4.

Performance Considerations

Routing traffic through an additional server and encrypting and decrypting it introduces some overhead. Performance therefore depends on factors including server location, available bandwidth, network congestion, and protocol efficiency. A nearby, well-provisioned VPN server will generally perform better than a distant or congested one.

Modern VPN technology is highly efficient, however, and under typical conditions the performance impact may be modest for everyday browsing, streaming, video conferencing, or remote work.

Part II: What Users Should Know

3. Understanding Privacy

Privacy is one of the primary reasons individuals use virtual private networks, but it is also one of the most misunderstood aspects of the technology. VPNs can meaningfully improve privacy, but they do not provide complete anonymity or prevent every form of online tracking.

Understanding what a VPN does—and does not—protect is essential to making informed decisions about privacy online.

What Information Exists Before a VPN?

Every time a device connects to the Internet, information about that connection is created as a natural consequence of how networks communicate. An Internet service provider (ISP) knows that a connection exists because it provides that connection. Websites receive an IP address so they know where to send their responses. Routers use addressing information to move packets toward their destinations.

Internet activity can also generate information beyond the content of communications themselves, including connection times, device characteristics, account logins, cookies, advertising identifiers, and other technical details. Some of this information is necessary for services to function; other information may support security, analytics, advertising, or tracking.

Metadata and Content

Understanding online privacy requires distinguishing between two different types of information: content and metadata. Content refers to the substance of a communication, such as the text of an email, the voice in a video call, the document being downloaded,

or the web page being viewed. Metadata is information about the communication rather than the communication itself, such as when a connection occurred, the devices involved, how long the session lasted, the amount of data transferred, and the network addresses used to deliver the communication.

Both forms of information have value, but they serve different purposes. A VPN primarily protects communications while they are in transit and changes who has visibility into certain metadata. It does not eliminate metadata altogether, nor could the Internet function if it did.

Recognizing this distinction helps avoid many of the misunderstandings surrounding online privacy.

What a VPN Can Mask

A VPN changes one important aspect of how Internet traffic is observed.

Instead of connecting directly from your Internet connection to the websites and services you use, traffic routed through the VPN first travels through an encrypted connection to the VPN provider. Your ISP can generally see that you are communicating with a VPN server, along with information such as the timing and volume of traffic, but it ordinarily cannot see the destinations carried inside the encrypted tunnel. A VPN masks the user's public IP address from the destination service, which generally sees the VPN server's address instead.

This additional layer of separation makes it more difficult to associate Internet activity directly with a particular residential or business connection. It can also provide meaningful protection on public Wi-Fi networks or in other environments where users may have limited control over the surrounding infrastructure.

Importantly, a VPN protects information while it is in transit. It changes who can observe certain aspects of the communication, but it does not eliminate all visibility into a user's online activity.

Limits of VPN Privacy and Security

One of the most common misconceptions about VPNs is that they make users anonymous.

A VPN does not erase identity. If you sign into your email, bank, social media account, or another online service, that service can still identify you through your account. Websites may also recognize returning visitors through cookies, browser characteristics, or other identifiers regardless of whether a VPN is being used.

The VPN connection itself does not prevent malware, phishing, weak passwords, or other threats that occur outside the network connection it protects. Some VPN services include additional security or built-in features, such as malware or phishing protection. These are separate capabilities whose availability and effectiveness depend on the service. VPNs address particular privacy and security risks; they are one layer of cybersecurity, not a substitute for the others.

DNS Privacy

As described in Chapter 2, the Domain Name System (DNS) functions as the Internet's address book. Every time a user visits a website, a DNS request typically occurs before any connection can be established.

Historically, DNS requests were commonly transmitted without encryption, making them visible to Internet service providers (ISPs) and other network operators along the relevant path. Encrypted DNS technologies such as DNS over HTTPS (DoH) and DNS over TLS (DoT) can protect those requests in transit, and many VPN providers route DNS requests through resolvers provided as part of the VPN service.¹⁶

Even so, encrypted DNS remains only one component of online privacy. Protecting DNS queries is valuable, but it should be understood as part of a broader security architecture rather than a complete privacy solution on its own.

Browser Fingerprinting, Cookies, and Account Tracking

Modern websites can recognize users in many ways that have nothing to do with IP addresses. Browsers reveal information about operating systems, screen sizes, installed fonts, language settings, time zones, and supported features. Individually these characteristics appear ordinary, but collectively they can create a highly distinctive fingerprint that allows websites to recognize returning visitors even if their IP address changes.¹⁷

Cookies—stored in browsers—allow websites to remember user preferences, shopping carts, authentication sessions, and other information between visits. They also allow services to recognize users who have previously signed in, regardless of whether a VPN is being used.

For these reasons, using a VPN alone does not prevent websites from recognizing users who choose to identify themselves through accounts or who permit persistent tracking technologies.

Privacy Is Not the Same as Anonymity

Privacy and anonymity are related concepts, but they are not the same. Privacy generally refers to limiting unnecessary observation or collection of information. Anonymity refers to making it difficult to associate actions with a particular individual.

A VPN can improve privacy by reducing the information visible to certain parties and separating Internet activity from a user's residential or enterprise connection. It may contribute to anonymity in some circumstances by masking the user's original IP address,

¹⁶ P. Hoffman & P. McManus, *DNS Queries over HTTPS (DoH)*, RFC 8484 (2018), <https://www.rfc-editor.org/rfc/rfc8484>; Z. Hu et al., *Specification for DNS over Transport Layer Security (TLS)*, RFC 7858 (2016), <https://www.rfc-editor.org/rfc/rfc7858>.

¹⁷ Peter Eckersley, *How Unique Is Your Web Browser?*, Privacy Enhancing Technologies Symposium (PETS) (2010), <https://coveryourtracks.eff.org/static/browser-uniqueness.pdf>.

but anonymity depends on many additional factors, including account usage, browser behavior, device configuration, and operational security.

VPNs are tools that protect communications in transit and give users greater control over what information about their Internet activity is exposed, and to whom. While they do not make users invisible, they strengthen the security and privacy of communications traveling across the Internet.

4. Information Collection, Logs, and Data Retention

Few phrases appear more frequently in VPN advertising than “no logs.” It is often presented as a promise that a provider knows nothing about its users and therefore has nothing to disclose if asked. The reality is more nuanced.

Every Internet service generates some operational information simply by functioning. The important questions are what information is collected, why it is collected, how long it is retained, who can access it, and whether it can reasonably be linked to individual users. Those distinctions shape both the privacy a service provides and the information potentially available in response to security incidents or lawful requests.

What Does “No Logs” Actually Mean?

Contrary to popular belief, “no logs” is not a technical standard. There is no universally accepted definition, no certification that automatically guarantees compliance, and no single architecture that every provider follows.

Instead, providers generally use the phrase to mean that they do not retain records of users’ browsing activity or other information that would allow their Internet activity to be reconstructed from provider records.

That does **not** necessarily mean the provider collects no information whatsoever. Most providers maintain at least some operational data necessary to authenticate users, troubleshoot technical problems, prevent abuse, process billing, or maintain the reliability of their services.

Providers remain subject to applicable legal obligations, which vary by jurisdiction and service. Where those obligations require particular account or payment information, that should not be conflated with a requirement to retain records of users’ online activity.

For consumers, the phrase “no logs” should therefore be viewed as the beginning of a conversation rather than the end of one. Understanding exactly what is and is not retained is far more informative than relying on a marketing slogan alone.

Understanding Different Types of Logs and Records

Discussions of VPN privacy often group different kinds of records under the term “logs.” This report distinguishes those records by what they contain and how they are used. Account and payment information should not be treated as equivalent to records of connections or online activity.

Authentication records, often called authentication logs, may record successful or unsuccessful sign-ins. Connection records, often called connection logs, may record when a VPN session began and ended or which server was used. Bandwidth and diagnostic data can help providers manage capacity, identify abuse, troubleshoot failures, or improve performance.

Activity records, often called activity or traffic logs, are different because they can describe what users actually did while connected, such as destinations or services accessed. These records receive the greatest attention in privacy discussions and are the type of information that “no logs” providers generally commit not to retain.

Recognizing these distinctions allows users to evaluate privacy practices with far greater precision than broad marketing claims alone.

Designing Systems That Know Less

Over the past decade, many VPN providers have redesigned their infrastructure around a simple engineering principle: the less information a system retains, the less information exists to compromise, misuse, or disclose.

Some providers have adopted architectures specifically designed to minimize the amount of user information their systems retain. Rather than relying on promises alone, these systems are intentionally designed so that little or no information about customer activity persists beyond what is operationally necessary to provide the service.

One approach involves operating VPN servers from volatile memory, or RAM, rather than relying on persistent local storage.¹⁸ Volatile memory loses its contents when power is removed. Avoiding persistent local storage can therefore reduce the amount of information that persists on individual servers. RAM-based infrastructure does not by itself guarantee privacy, but when combined with broader data-minimization practices it can reduce the amount of sensitive information available to compromise, misuse, or disclose.

These architectural decisions demonstrate an important point: privacy is not achieved solely through policy. It is often—and increasingly—achieved through engineering.

¹⁸ Will Shanklin, *ExpressVPN's External Auditors Confirm No-Logs Policy as of February*, Engadget (2025), <https://www.engadget.com/cybersecurity/vpn/expressvpns-external-auditors-confirm-no-logs-policy-as-of-february-171957335.html>; see also NIST, Volatile Memory, Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/volatile_memory.

Verifying Privacy Claims

Because users cannot directly inspect a provider's internal systems, trust depends more and more on independent verification.

VPN providers may commission third-party firms to assess their infrastructure, information collection and retention practices, and operational controls.¹⁹ Depending on their scope, these assessments can examine source code, infrastructure, operational controls, or the consistency of privacy claims with deployed systems. Their conclusions apply to the versions, systems, and periods examined.



Transparency reports have become another important accountability mechanism.²⁰ These reports summarize government requests for information, explain how providers responded, and often disclose whether any responsive information existed in the first place.

None of these mechanisms guarantees perfect privacy. Together, however, they provide users with additional tools for evaluating whether a provider's technical architecture aligns with its public commitments.

When Information Must Be Retained

Information collection and retention practices are shaped not only by engineering decisions, but also by legal obligations.

Many jurisdictions require companies to retain certain categories of business records for financial, tax, or regulatory purposes. Some governments impose data retention requirements on telecommunications providers or other communications services, although whether and how those laws apply to VPN providers varies considerably from one jurisdiction to another.

Similarly, providers may receive lawful requests for information through warrants, subpoenas, or court orders. A provider must respond in accordance with the laws of the jurisdictions in which it operates.

A lawful demand can only result in disclosure of information the provider possesses or controls. That is why retention decisions are not simply an engineering preference; retention decisions help determine what information may ultimately be available in response to the legal process.

¹⁹ Shanklin, *supra* note 18. For a technical example, see Cure53, *Mullvad VPN Relay Infrastructure: Penetration Test and Source Code Audit* (June 2024), https://cure53.de/pentest-report_mullvad_2024_v1.pdf.

²⁰ See, e.g., Proton VPN, *Proton VPN Transparency Report and Warrant Canary*, <https://protonvpn.com/blog/transparency-report>.

Marketing Claims and Technical Reality

The VPN industry has grown rapidly, and competition has encouraged providers to emphasize privacy as a defining feature of their services. While many companies have invested heavily in engineering systems that genuinely minimize data retention, marketing language has not always kept pace with technical reality.

Claims such as “100 percent private,” “zero tracking,” or other absolute privacy guarantees often lack precise qualifications and can create unrealistic expectations about what VPNs can accomplish. Consumers should view these claims with healthy skepticism given the operational-data realities described above. They should instead look for concrete evidence such as published privacy policies, independent audits, transparency reports, and clear explanations of information collection and retention practices.

The goal is not to identify a provider that promises the most, but one that explains its practices honestly, designs its systems thoughtfully, and demonstrates a commitment to accountability. Ultimately, trust is earned through architecture, transparency, and consistent operational practice and performance, not through slogans.

5. Jurisdiction Matters

One of the most common questions people ask when choosing a VPN provider is, “Where is the company based?” It is a reasonable question, but an incomplete one.

A VPN provider may be incorporated in one country, employ staff in another, operate or lease infrastructure in dozens more, and serve users around the world. Those jurisdictions may impose different legal obligations affecting how the service operates and what information may be collected, retained, or disclosed. Understanding a VPN therefore requires looking beyond corporate headquarters to the broader legal environment in which the service operates.

Corporate Domicile Is Only Part of the Story

Corporate domicile matters, but it is only one part of a provider’s legal environment. VPN providers may operate infrastructure in multiple countries and rely on data centers, cloud platforms, payment processors, contractors, and other service providers operating under different legal frameworks.

The relevant question is therefore not simply where a VPN company is headquartered, but which jurisdictions and legal relationships affect the particular service being provided.

Data Sovereignty and Localization

Many governments have adopted laws governing where certain categories of data may be stored, processed, or transferred.²¹ Chapter 11 examines examples of such government action. Data localization requirements may require particular information to remain within a country or be processed under specified conditions, while the broader concept of data sovereignty concerns the legal authority governing data. Chapter 10 examines some of the policy motivations behind these approaches; the focus here is what they mean for how a provider operates.

Data-localization and related requirements vary by jurisdiction, service, and category of information. A requirement applying to one type of provider or data should not be assumed to apply to every VPN service.

Where they apply to a VPN provider, these rules can create operational challenges. A provider may wish to maintain a globally distributed network while also complying with local requirements governing user information, financial records, or operational data. Some providers respond by limiting—or withdrawing—the services they offer in particular countries, while others redesign their infrastructure to minimize the information that must be retained in any single jurisdiction. These decisions are shaped by the interaction between engineering, law, and public policy.

Government Requests for Data

Governments use court orders, subpoenas, warrants, and other legal processes to seek information from private companies. When investigations cross borders, authorities may also rely on international mechanisms, including Mutual Legal Assistance Treaties (MLATs), to seek evidence located in another jurisdiction.²² As discussed in Chapter 4, many technology companies, including numerous VPN providers, publish transparency reports describing the number and types of government requests they receive.

For a VPN provider, two questions are particularly important: what does applicable law require, and what information does the provider actually possess or control? A provider located outside a country is not necessarily beyond its legal reach, while incorporation within a country does not by itself determine every obligation. Technical architecture and data-retention practices therefore matter alongside jurisdiction when assessing what information may be available through legal process.

²¹ Elena Del Giovane, Janos Ferencz & Javier López González, *The Nature, Evolution and Potential Implications of Data Localisation Measures*, OECD Trade Policy Papers No. 278 (2023), https://www.oecd.org/en/publications/the-nature-evolution-and-potential-implications-of-data-localisation-measures_179f718a-en.html.

²² U.S. Department of Justice, Criminal Division, Office of International Affairs, *Mutual Legal Assistance Treaties of the United States* (Apr. 2022), <https://www.justice.gov/criminal/criminal-oia/file/1498806/dl?inline=>.

Choosing Jurisdiction Through a Risk Lens

There is no universally “best” jurisdiction for every VPN user. A multinational corporation protecting proprietary information faces different risks from a journalist working in an authoritarian country, a healthcare provider subject to regulatory requirements, or an individual seeking greater privacy on public networks.

Jurisdiction should therefore be considered as one part of a broader assessment that includes technical architecture, data-retention practices, transparency, governance, and the particular risks a user is trying to address. The next chapter brings these factors together into a practical framework for choosing a VPN provider.

6. Choosing a VPN

Choosing a VPN is fundamentally an exercise in trust. By routing traffic through a VPN, a user changes which parties occupy positions of visibility within the connection and places new trust in the organization operating the service.

Providers differ in their technical architecture, business models, operational practices, and legal environments. Evaluating one therefore requires looking beyond features and marketing claims to understand how the service is built, operated, and governed.

Understanding the Business Model

Operating a VPN service requires servers, bandwidth, engineering, security, customer support, and ongoing maintenance. Free services are not inherently untrustworthy, nor are paid services automatically deserving of trust. The relevant question is how the provider sustains its operations and whether its incentives align with users’ privacy and security expectations.

Evaluating the Software and the Network

Providers differ in how they develop their software and operate their infrastructure. Some publish open-source clients, while others use proprietary applications. More important than the licensing model itself is whether the provider demonstrates secure development practices, regular updates, responsible vulnerability management, and transparency about how its software and infrastructure are secured.

Network design matters as well. Geographic distribution, capacity, redundancy, and infrastructure management all affect performance and resilience. Users should consider whether a provider operates where they need it and provides meaningful information about how its network is managed and secured.

Assessing Trustworthiness

The central question is simple: why should a user trust the organization operating the VPN?

Jurisdiction, information collection and retention practices, technical architecture, independent audits, transparency reporting, and corporate governance all contribute to the answer. Providers that explain their practices and limitations clearly, minimize unnecessary data collection, and provide independent evidence supporting their claims give users a stronger basis for informed trust than those relying primarily on marketing promises. Untrustworthy VPN services can undermine user privacy through weak encryption, activity logging, or misuse of user data.²³

Reviewing Security Features

Features such as kill switches, split tunneling, multi-hop routing, and protocol selection can improve security or usability in particular circumstances. Their importance depends on the user's risk.

A human rights activist operating in a high-risk environment, for example, may depend on a kill switch to prevent a dropped VPN connection from unexpectedly exposing network information. The same feature may be far less consequential for a family seeking additional privacy while traveling. Features should therefore be evaluated according to the problem they solve rather than treated as a universal checklist.

Choosing Based on Your Needs

There is no single VPN that is right for every user or circumstance. A traveler seeking additional privacy has different requirements from a journalist protecting sources, an employee accessing corporate systems, or an organization connecting infrastructure across multiple locations.

A useful evaluation begins with two sets of questions:

What do I need from the VPN?

- What am I trying to protect and from whom?
- Where and how will I use the service?
- What would happen if the protection failed?
- Do I need access to particular server locations or support for particular devices?
- Do I need to use specific protocols or additional security features?

Why should I trust this provider?

- What information does it collect and retain?
- What jurisdictions affect the service?

²³ Internet Society, *Policy Brief: VPN Restrictions* (Sept. 2026), <https://www.internetsociety.org/resources/policybriefs/2026/vpn-restrictions/>.

- How does it secure and operate its infrastructure?
- Are its claims supported by audits, transparency reporting, or other independent evidence?

The goal is not to identify a universally “best” VPN, but to determine whether a provider’s technology, practices, and trust model match the security and privacy problems the user is trying to solve.

Separating Facts from Marketing

Evaluate a provider’s marketing claims against what VPN technology actually does:

- A VPN technology protects communications across networks outside the user’s control. It does not automatically replace protections against malware, phishing, weak passwords, or other security risks. Some VPN services include additional or built-in security features, such as malware or phishing protection.
- As Chapter 3 explains, a VPN does not erase identity: account logins, cookies, and browser fingerprinting can still identify or recognize users.
- Providers should substantiate their privacy and security claims. Bundled antivirus, password managers, and other security tools serve separate functions; their capabilities should not be attributed to the VPN itself.

Part III: The Role of VPNs in a Secure Internet

7. Protecting People, Not Just Networks

Much of this report has focused on VPNs as cybersecurity infrastructure, but cybersecurity ultimately exists to protect people.

Individuals use VPNs for many of the same reasons organizations do: to communicate securely across networks they do not control and to reduce unnecessary exposure of sensitive information. Public debate often focuses on circumvention or misuse, but understanding the legitimate reasons why people want to protect their communications is equally important to understanding the role VPNs play in the modern Internet.



Emerging Trust Frameworks

One development in recent years has been the emergence of voluntary trust frameworks designed to help users evaluate VPN providers against consistent operational and governance criteria. Rather than relying solely on marketing claims, these initiatives seek to establish common expectations around transparency, security practices, accountability, and responsible stewardship.

The **VPN Trust Initiative (VTI) Trust Seal** is one example of this approach. By providing a structured framework through which participating providers can demonstrate adherence to recognized operational and privacy practices, initiatives like the VTI Trust Seal aim to strengthen user confidence while encouraging greater transparency across the industry.

No certification should replace informed evaluation. Instead, trust frameworks are most valuable when they complement independent audits, transparent governance, and a provider’s demonstrated commitment to responsible operation.

A 2022 study of VPN users in the United States found that privacy and security were primary motivations among its general-user sample, while university students also emphasized access to content.²⁴

Protecting Personal Privacy

Most people who benefit from secure Internet connections are not journalists working with confidential sources or activists operating under repressive governments. They are ordinary Internet users conducting ordinary activities across networks they do not necessarily control.

People check bank accounts from hotels, access work systems while traveling, make purchases from airports, manage healthcare information from coffee shops, and communicate with family members while connected to shared or public networks. They routinely transmit passwords, financial information, personal communications, and other sensitive data across infrastructure operated by third parties.

Many of the services people use already protect these communications through encryption and other security measures. Banks use encrypted connections and fraud-detection systems. Websites increasingly use HTTPS (Hypertext Transfer Protocol Secure), which encrypts information in transit between the browser and website. Devices and applications incorporate their own security protections. A VPN does not replace any of these safeguards or prevent every form of fraud, interception, or tracking.

Instead, it adds another layer of protection at the network level. By encrypting traffic between the user's device and a trusted VPN server, a VPN can reduce the information exposed to operators or other observers on networks the user does not control. This protection can also make it harder for attackers on the local network to intercept or tamper with that traffic. This can be particularly valuable when people rely on public and shared Internet connections where they may know little about how the network is configured, secured, or operated.

These are not unusual or specialized circumstances. They are part of ordinary digital life. People increasingly work, bank, shop, communicate, travel, and access sensitive services from many different locations and across many different networks. VPNs give individuals an additional security and privacy tool for doing those things with greater confidence and greater control over the information their network connection exposes.

²⁴ Agnieszka Dutkowska-Zuk et al., *How and Why People Use Virtual Private Networks*, 31st USENIX Security Symposium 3451–65 (2022) (reporting interviews with 32 university students and surveys of 349 university students and 348 general VPN users in the United States), <https://www.usenix.org/conference/usenixsecurity22/presentation/dutkowska-zuk>.

Protecting Journalism, Human Rights, Academic Freedom, and Political Expression

Journalists conduct sensitive research and communicate with confidential sources. Human rights organizations document abuses and assist vulnerable communities. Individuals may engage in political expression where doing so carries personal, professional, or legal risk. Researchers, students, and academics explore controversial or politically sensitive subjects as part of legitimate scholarly work.

These users may have a particular need to limit unnecessary observation of their communications, their location, or the people and resources with which they interact. VPNs are one component of the broader digital security practices they may rely upon, not a substitute for legal protections or democratic institutions, but a meaningful layer of protection for both the free flow of information and the people participating in it.²⁵

Protecting Vulnerable Individuals

Not every privacy concern involves governments or major institutions. Survivors of domestic violence or child abuse, and other victims of crime, may need to communicate without unnecessarily exposing their location or conversations.²⁶ Members of vulnerable communities may want to seek information or communicate with others without unnecessary observation. People seeking sensitive health information or legal advice may similarly wish to limit how broadly those activities are exposed.

In these circumstances, privacy is not an abstract principle. It can be a practical component of personal safety.

Privacy Is Not Evidence of Wrongdoing

The desire to limit unnecessary exposure should not be treated as inherently suspicious. Organizations protect confidential business information, governments secure sensitive communications, financial institutions safeguard customer records, and hospitals protect medical information because those communications deserve appropriate security.

Individuals have legitimate reasons to seek similar protections. Limiting unnecessary exposure can reduce risk, preserve confidentiality, protect personal safety, and support the exercise of fundamental rights. VPNs do not provide absolute anonymity or immunity from lawful investigation, or complete protection from all hacking and security breaches. They provide one means through which individuals can exercise greater control over the information exposed as they participate in digital life.

²⁵ Defenders Protection Initiative, *Secure & Defend: A Toolkit for Activists & Defenders* (2026), <https://www.defendersprotection.org/wp-content/uploads/2026/03/SECURE-DEFEND-A-TOOLKIT-FOR-ACTIVISTS-DEFENDERS-DPI-TOOLKIT-V1.0.pdf>.

²⁶ National Network to End Domestic Violence, Safety Net Project, *WiFi Safety & Privacy: Tips for Victim Service Agencies and Survivors*, <https://www.techsafety.org/wifi-safety-privacy-tips-for-survivors>.

8. VPNs as Critical Cybersecurity Infrastructure

For many people, VPNs are associated primarily with personal privacy, public Wi-Fi, or accessing services across geographic boundaries. Those are legitimate uses, but they represent only one part of a security technology deeply embedded in the operation of the modern Internet.

As Chapter 1 explained, VPNs were originally developed to connect employees, offices, and infrastructure securely across the public Internet. This chapter looks at how that technology functions as cybersecurity infrastructure today across businesses, governments, and other institutions.

Securing a Modern Workplace

Modern organizations maintain sensitive financial information, customer data, intellectual property, administrative systems, operational technology, and other resources that should not be broadly exposed to the public Internet. At the same time, remote work, mobile workforces, and globally distributed teams require authorized users to reach those resources from outside traditional corporate networks.

VPNs provide one mechanism through which authorized employees, contractors, and partners can reach protected systems, regardless of their physical location. Users authenticate before a connection is established, and access can be limited according to role, device, location, or business need. VPNs do not replace identity management, multifactor authentication, endpoint protection, firewalls, network segmentation, or monitoring. They work alongside those safeguards as part of a layered security architecture.²⁷

Newer approaches, including Zero Trust Network Access, supplement or replace traditional VPN deployments in some environments by providing more granular access controls.²⁸ But the underlying security requirement remains: protecting communications across untrusted networks and controlling access to protected resources.

Connecting Offices, Data Centers, and Cloud Infrastructure

VPNs are not limited to connecting individual employees. Organizations establish encrypted connections among offices, manufacturing facilities, data centers, cloud environments, and other infrastructure. They may also provide controlled access to suppliers, contractors, consultants, and managed service providers that need to reach selected systems. These connections allow geographically distributed users and networks to communicate securely without broadly exposing internal resources to the public Internet.

²⁷ National Security Agency & Cybersecurity and Infrastructure Security Agency, *Selecting and Hardening Remote Access VPN Solutions* (Sept. 28, 2021), https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF.

²⁸ Scott Rose et al., *Zero Trust Architecture*, NIST SP 800-207 (2020), <https://csrc.nist.gov/pubs/sp/800/207/final>.

Securing Public and Shared Networks

Public Internet access is now available in coffee shops, hotels, airports, conference venues, libraries, and many other shared environments. These networks enable mobility and productivity, but they are generally outside the user's control. VPNs provide an additional layer of protection by encrypting communications between a user's device and a trusted VPN server before the traffic travels across the broader Internet.

Encryption provided by websites and applications has substantially improved Internet security. A VPN is not a replacement for the encryption websites and apps already provide, but it reduces opportunities for local network observation and provides broader protection for traffic leaving the device.

One Technology, Many Deployment Models

The term VPN encompasses several deployment models. A company may operate its own VPN infrastructure for employees. Two offices may be joined through a site-to-site tunnel. A cloud provider may offer VPN connectivity between customer environments. A consumer VPN service may operate a global network through which individual users route Internet traffic.

Consumer VPN services include both paid subscriptions and services offered free of charge. These business models can create different incentives around data collection, advertising, and user privacy. Evaluating a provider therefore requires understanding how the service is funded and whether its practices align with its privacy and security commitments.

These deployments differ in who operates them, who is authorized to connect, where traffic ultimately travels, and the relationship between the user and operator. They may also be treated differently under law and regulation. At the network level, however, they can rely on many of the same protocols and mechanisms for authentication, encryption, and tunneling across untrusted networks.

Distinguishing consumer and enterprise deployments helps explain how VPNs are used; it does not, by itself, establish that they require separate regulatory regimes. Appropriate obligations should reflect the activity being regulated, the provider's role and capabilities, and the applicable legal framework.

That technical overlap becomes important when regulation moves beyond the business practices of a particular commercial provider and toward the underlying network. Measures that attempt to identify or block VPN traffic based on protocols, ports, IP addresses, or other observable characteristics may be less able to distinguish among different uses of the same technology. Requirements imposed on data centers, cloud providers, or other intermediaries supporting VPN services can likewise extend beyond the provider directly being regulated.

This does not mean that every restriction on a consumer VPN service will affect enterprise VPNs. The consequences depend on how a policy is designed and where it is implemented. But policymakers should understand both the deployment model they intend to regulate and the technical layer at which they propose to intervene.

Why This Matters for Policy

Consumer VPN services should neither be treated as identical to enterprise VPN deployments nor as technologically unrelated to them. They belong to the same broader family of secure networking technologies and rely on many of the same foundational capabilities.

That distinction becomes important for policy. The more precisely regulation targets a particular service, provider, or harmful activity, the easier it may be to distinguish among different uses. The closer intervention moves toward shared protocols and underlying Internet infrastructure, the greater the need to consider effects beyond the activity policymakers originally intended to address.

9. VPN Critics and Infrastructure Neutrality

Few topics generate more debate around VPN technology than circumvention. Critics frequently characterize VPNs as mechanisms for bypassing laws, platform restrictions, or government controls, while supporters emphasize their role in privacy, cybersecurity, and access to information.

Both uses are possible because the technology itself does not determine intent. A VPN establishes an encrypted connection across an untrusted network. How that capability is used depends on the user.

Circumvention and Censorship Resistance

Because VPNs can change the apparent origin of Internet traffic and route communications around certain network restrictions, they may allow users to reach content or services that would otherwise be inaccessible due to geographic content restrictions, organizational policies, or government-imposed restrictions.

That capability can be viewed very differently depending on the context. A government enforcing Internet restrictions may regard VPN use as circumvention, while a journalist, human rights defender, or ordinary citizen in a censored environment may regard the same capability as essential to accessing information or communicating securely. The technology is the same. The purpose, legal context, and consequences of its use are very different.

The Neutrality of Internet Infrastructure

Much of the Internet depends on general-purpose infrastructure that performs technical functions without determining the intent behind every communication it enables. Routers forward packets, DNS resolvers translate names into addresses, cloud providers supply computing and storage, and Internet service providers transport communications for enormous numbers of lawful users.

VPNs occupy a similar position. They provide a secure communications capability that can support many different activities. The technology itself does not determine whether a particular use is lawful, ethical, or appropriate.

This does not mean infrastructure providers have no responsibilities for activities occurring through their services. It does mean that imposing responsibility on general-purpose infrastructure requires careful consideration of what the provider can reasonably know, control, and address without disrupting unrelated legitimate uses, or the fundamental architecture of the Internet.

Why Infrastructure Neutrality Matters

Governments may legitimately impose obligations on technology providers to address specific harms, comply with lawful investigations, or meet appropriate security requirements. The policy challenge is determining where those obligations should fall and how precisely they can be implemented.



Technology Does Not Determine Intent

Almost every widely used communications technology can be employed for both legitimate and illegitimate purposes. Encrypted messaging protects family conversations, confidential business negotiations, and attorney-client communications, but it may also be misused by criminals. Cloud storage enables collaboration among businesses and researchers while also being capable of storing unlawful material. VPN capabilities likewise support both lawful uses and misuse.

This distinction has long been recognized in technology policy. In *Sony Corp. of America v. Universal City Studios*, the U.S. Supreme Court held that distributing a technology capable of substantial non-infringing uses did not, without more, establish contributory copyright infringement liability simply because the technology could also be used for infringement.²⁹

VPNs have well-established legitimate uses across business, education, healthcare, journalism, government, and personal cybersecurity. Evaluating the technology solely through the lens of potential misuse therefore risks overlooking the many lawful activities that depend upon the same capabilities. Individuals' security and privacy interests should not be discounted simply because they use consumer services rather than institutional VPN deployments. Businesses, governments, and other institutions continue to use—and in many cases require³⁰—VPNs to protect sensitive information.

²⁹ *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), <https://supreme.justia.com/cases/federal/us/464/417/>.

³⁰ National Cyber Security Centre, *Virtual Private Networks (VPNs)*, in Device Security Guidance, <https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks>.

Restrictions directed at conduct are not necessarily equivalent to restrictions directed at the general-purpose technology used to carry it out. This distinction becomes particularly important when intervention moves deeper into Internet infrastructure, where technical measures intended to affect one category of use may also affect unrelated users and services.

The chapters that follow examine how governments have approached that challenge in practice, including measures directed at VPN providers, users, distribution channels, and the underlying network itself.

Part IV: VPNs Under Pressure

10. Why Governments Are Regulating VPNs

Governments with markedly different political systems, legal traditions, and policy priorities have proposed or adopted measures affecting VPN providers and VPN use. Their motivations range from cybersecurity, national security, and criminal investigations to child protection, copyright enforcement, data sovereignty, and control over access to information.

Understanding those motivations is essential to evaluating VPN regulation. The debate reflects broader questions about how societies balance cybersecurity, privacy, public safety, economic interests, and individual rights in an interconnected digital environment.

Policy Objectives Cited in VPN Debates

Law enforcement agencies investigate cybercrime, ransomware, fraud, child exploitation, and threats to national security. Policymakers must also address questions involving age assurance, copyright enforcement, data sovereignty, and access to information.

Governments cite different objectives when considering measures affecting VPNs. These objectives are not equivalent: some concern specific unlawful conduct, while others concern restrictions on access to information. The following list describes those policy debates; it does not establish that VPNs cause the underlying harm or that restricting VPNs is an effective or proportionate response.

- **National security:** Governments may be concerned about cyber espionage, terrorism, hostile state activity, or technologies that make attribution and network-based investigations more difficult.
- **Criminal investigations and lawful access:** VPN services that minimize retained information or obscure network location may complicate investigations that rely on provider records or network attribution.
- **Protecting children and age verification:** VPNs may allow users to appear to connect from another jurisdiction if they connect through a VPN server with an IP address in another jurisdiction.

- **Copyright and commercial enforcement:** VPNs may complicate efforts to identify users engaged in infringement or enforce geographic licensing restrictions.
- **Data localization and digital sovereignty:** Governments may scrutinize services that route communications across national borders or through infrastructure located in other jurisdictions.
- **Information control:** Governments that filter Internet access or restrict particular services may target VPNs because they can make those restrictions more difficult to enforce.

The capabilities discussed here also support secure communications, user privacy, and access to information. Evaluating a proposed response therefore requires examining the specific harm, the evidence that the harm is real and material, the evidence that the measure would address it, and its effects on lawful users and the security functions described earlier in this report.

A Broader Debate Over Internet Intermediaries

VPN regulation also reflects a broader development in Internet policy.³¹ Governments increasingly look beyond the individuals engaged in particular conduct toward the intermediaries that make digital activity possible. Internet service providers, cloud and hosting providers, domain name operators, and payment processors have all faced growing expectations to help achieve public policy objectives. VPN providers are increasingly part of that discussion.

This raises a larger question about where responsibility should fall within the Internet ecosystem. An intermediary may have the technical ability to observe, restrict, or interrupt some activity without necessarily being the actor best positioned to understand or address the underlying harm.

The question is therefore not simply whether Internet intermediaries should ever have responsibilities. It is whether particular obligations are directed toward actors with meaningful knowledge of and sufficient control over the activity being regulated. Can those obligations be implemented without creating disproportionate consequences and collateral damage elsewhere in the Internet ecosystem? Could these obligations produce repeated temporary fixes that are easily circumvented?

³¹ See i2Coalition, *DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet* (2025), <https://i2coalition.com/wp-content/uploads/2025/05/DNS-at-Risk-How-Network-Blocking-and-Fragmentation-Undermine-the-Global-Internet.pdf>; i2Coalition, *Intermediary Liability*, <https://i2coalition.com/intermediary-liability/>. These sources address infrastructure-level enforcement and intermediary responsibility rather than every service category listed here.

Setting the Stage

These motivations explain why VPNs have entered policy debates around the world. They do not tell us how governments have chosen to intervene.

The following chapter examines case studies covering several different approaches, ranging from data-retention and licensing requirements to blocking orders, circumvention penalties, distribution controls, and network-level interference.

11. Case Studies

VPN regulation does not follow a single model. Governments have approached VPNs through data-retention requirements, provider licensing, website-blocking obligations, restrictions on circumvention, controls on VPN distribution, and technical interference with VPN traffic itself.³²

The following case studies illustrate several of these approaches. They are not intended as a comprehensive survey of global VPN regulation, but as examples of how different policy objectives can produce dramatically different interventions in the same general-purpose security technology.



India: Mandatory Data Retention Changes the Infrastructure

India's policy provides one of the clearest examples of how VPN regulation can affect the way services are technically operated.

In April 2022, the Indian Computer Emergency Response Team (CERT-In) issued cybersecurity directions requiring VPN service providers, along with data centers, cloud providers, and virtual private server providers, to retain specified customer information for five years. The required information included names, addresses, contact information, subscription periods, IP addresses, and the stated purpose for using the service. CERT-In also imposed broader requirements to retain certain system logs for 180 days.³³

Importantly, CERT-In subsequently clarified that the VPN-specific requirements did not apply to enterprise or corporate VPNs. They applied to providers offering what CERT-In described as “Internet proxy like services” using VPN technology to general Internet users.³⁴

³² Internet Society, *supra* note 23.

³³ Carl Gahnberg et al., *Internet Impact Brief: India CERT-In Cybersecurity Directions 2022*, Internet Society (2022), <https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-india-cert-in-cybersecurity-directions-2022/>.

³⁴ American Bar Association, *May 2022 in Brief: Internet Law & Cyber-Security*, Business Law Today (May 2022), https://www.americanbar.org/groups/business_law/resources/business-law-today/2022-may/month-in-brief-internet-law-cyber-security/.

That distinction limited the direct reach of the rule, but it created a fundamental conflict for commercial providers whose services had been designed specifically to minimize retained user information. Rather than redesign their systems to collect data they had previously chosen not to retain, several major providers removed physical VPN servers from India. ExpressVPN, Surfshark, and NordVPN were among the providers that withdrew Indian infrastructure.³⁵

The result illustrates an important distinction between banning a technology and regulating the conditions under which it can operate. India did not prohibit VPN use. Instead, its rules changed the data-retention obligations imposed on commercial VPN providers serving individual users. For some providers, that was enough to make operating physical infrastructure in the country incompatible with the architecture and privacy commitments of their services.

The Indian government's actions demonstrate how regulation can reshape Internet infrastructure even without directly restricting users' access to a technology. Requirements governing what providers must know, retain, and disclose can influence where infrastructure is located, which providers remain in a market, and how services are technically designed.



United Kingdom: Age Assurance and Proposals to Restrict VPNs

The UK case concerns proposals to restrict VPN access in response to age-assurance requirements, rather than an adopted VPN ban or age-gating requirement. It illustrates how regulation directed at online content can create pressure to regulate technologies users may employ to circumvent it.

Under the Online Safety Act, services providing or allowing certain categories of content must use highly effective age assurance to prevent children from accessing it.³⁶ As those requirements were implemented, policymakers increasingly raised concerns that children could use VPNs to bypass geographically based age checks. VPNs consequently became part of a broader debate about whether the effectiveness of online safety regulation required additional controls over circumvention technologies.³⁷

³⁵ Michael Kan, *NordVPN Joins Growing Number of VPNs Removing Servers From India*, PCMag (June 14, 2022), <https://www.pcmag.com/news/nordvpn-joins-growing-number-of-vpns-removing-servers-from-india>.

³⁶ UK Department for Science, Innovation and Technology, *Online Safety Act: Explainer* (2023), <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>.

³⁷ UK Parliament, *Online Safety Act 2023: Virtual Private Networks*, House of Lords Debate, Hansard (Sept. 15, 2025), <https://hansard.parliament.uk/Lords/2025-09-15/debates/57714CE6-0CE4-49F6-B028-E271D5100F7F/OnlineSafetyAct2023VirtualPrivateNetworks>.

That debate eventually produced proposals to regulate VPN access itself. In January 2026, the House of Lords approved an amendment to the Children’s Wellbeing and Schools Bill that would have required regulations prohibiting commercial consumer VPN services from being provided to children in the UK, potentially enforced through age assurance.³⁸

The government ultimately chose a different approach. Following research³⁹ into how children actually circumvent age restrictions – finding that VPNs are not widely used by children to avoid age checks – it announced in July 2026 that it would not ban or age-gate VPNs. Instead, it placed responsibility on regulated platforms to take stronger measures against circumvention and asked its communications services regulator, Ofcom, to study additional ways services could detect and mitigate VPN use. The government specifically cited the legitimate privacy, security, business, and freedom-of-expression uses of VPNs as well as concerns that restrictions could push children toward less accountable VPN services.⁴⁰ Ofcom’s research distinguishes general VPN use from use to access age-restricted content: children reported using VPNs for a range of purposes, including privacy.⁴¹

The UK debate demonstrates how proposals for regulation can move outward through the Internet stack. A policy initially directed at restricting children’s access to particular online content led to consideration of obligations on a general-purpose security technology because that technology could potentially be used to circumvent the original restriction. It also demonstrates the value of evidence before extending regulation to another layer of Internet infrastructure: the government ultimately concluded that VPN restrictions were not, on the available evidence, the appropriate response.



Pakistan: Registration, Licensing, and Government Control

Pakistan’s government has taken an increasingly regulatory approach to VPNs as part of broader efforts to control Internet access and distinguish what the government considers legitimate VPN use from circumvention.

The Pakistan Telecommunication Authority (PTA) has required organizations and other commercial users to register VPN connections, including by providing identifying information and IP addresses. During 2024, as the government restricted access to the social media platform X and Internet users increasingly relied on VPNs to reach blocked services,

³⁸ UK Parliament, *Children’s Wellbeing and Schools Bill: House of Lords Report Stage* (Jan. 2026), <https://www.parliament.uk/business/news/2026/jan-2026/childrens-wellbeing-and-schools-bill-house-of-lords-report-stage/>.

³⁹ UK Department for Science, Innovation and Technology, *Children’s Circumvention Behaviours Online* (2026), <https://www.gov.uk/government/publications/childrens-circumvention-behaviours-online/childrens-circumvention-behaviours-online>.

⁴⁰ UK Department for Science, Innovation and Technology, *Growing Up in the Online World: Government Response* (July 2026), <https://www.gov.uk/government/consultations/growing-up-in-the-online-world-a-national-consultation/outcome/growing-up-in-the-online-world-government-response-july-2026>.

⁴¹ Ofcom, *Experiences of Age Assurance, Use of VPNs, and Attitudes to the Protection of Children Measures* (July 2026), <https://www.ofcom.org.uk/online-safety/protecting-children/experiences-of-age-assurance-use-of-vpns-and-attitudes-to-the-protection-of-children-measures>.

the PTA expanded and streamlined this registration system for businesses, freelancers, banks, call centers, and other users.⁴²

The policy also demonstrated the tension between Internet controls and ordinary economic activity. Pakistan's technology industry warned in 2024 that Internet disruptions and unreliable VPN connectivity were interfering with business operations, particularly for companies dependent on secure connections to international customers and systems.⁴³

The Pakistani government subsequently moved from registering VPN connections toward licensing VPN providers themselves. In December 2024, the PTA announced that providers offering VPN services in Pakistan would be required to obtain a Class License for Data Services.⁴⁴ Licensing began in 2025, and the system was subsequently expanded under the Class Value Added Services regime. Under the newer model, users can obtain VPN services from licensed providers without separately registering their own IP addresses or mobile numbers with the PTA.⁴⁵

The actions taken by the Pakistani government illustrate how VPN regulation can evolve from controlling particular connections toward controlling the market through which VPN services are provided. VPNs remain available for authorized purposes, including the business and cybersecurity uses the government itself recognizes. But the regulatory framework increasingly determines which providers may offer those services and the conditions under which users may access them.

France: Copyright Enforcement Reaches VPN Providers

Copyright litigation in France provides a particularly direct example of obligations moving through judicial enforcement from unlawful content toward the general-purpose infrastructure.

In May 2025, the Paris Judicial Court ordered five major VPN providers—NordVPN, CyberGhost, Surfshark, ExpressVPN, and Proton VPN—to block access from France to 203 domain names associated with unauthorized streams of sporting events. The case was brought by Canal+ and concerned rights to competitions including the UEFA Champions League, Premier League, and Top 14.

⁴² Pakistan Telecommunication Authority, *VPN Registration Process* (Nov. 18, 2024), <https://pta.gov.pk/category/vpn-registration-process-55198854-2024-11-18>.

⁴³ International Trade Administration, U.S. Department of Commerce, *Pakistan — Internet Disruptions*, <https://www.trade.gov/market-intelligence/pakistan-internet-disruptions>.

⁴⁴ Pakistan Telecommunication Authority, *PTA Data Services Licensing* (Dec. 18, 2024), <https://pta.gov.pk/category/pta-resumes-granting-class-licenses-for-data-services-1060093500-2024-12-18>.

⁴⁵ Pakistan Telecommunication Authority, *PTA VPN Provider Licensing* (Nov. 13, 2025), <https://www.pta.gov.pk/category/pta-commences-licensing-of-vpn-service-providers-under-cvas-data-regime-1566349483-2025-11-13>.

The court treated VPN providers as intermediaries capable of being required to implement blocking measures even though they neither hosted nor operated the infringing services. The decisions are currently pending appeal.⁴⁶

The significance of the decision extends beyond the particular domains involved. French courts had already issued blocking orders against Internet access providers and other intermediaries to combat unauthorized sports streaming.⁴⁷ The 2025 decision extended that enforcement approach to VPN providers because users could employ VPN services to reach sites already subject to blocking elsewhere in the Internet access chain.

This was not a one-time development. French courts subsequently issued additional orders requiring VPN providers to block unauthorized streaming services, including services identified after the initial orders.⁴⁸

IP- and domain-based blocking can also affect lawful services that share an IP address or domain with targeted content.⁴⁹

These cases, brought by rightsholders before French courts, illustrate how obligations imposed at one layer of the Internet can migrate to another when users find alternative technical paths around court-ordered restrictions. The policy question therefore extends beyond which intermediaries can implement blocking orders to whether those measures effectively reduce infringement and what consequences they create for lawful users.



Brazil: Platform Blocking Extends to VPN Users

Brazil's policy illustrates how restrictions directed at an online platform can extend to the technologies individuals may use to reach it.

In August 2024, Justice Alexandre de Moraes of Brazil's Supreme Federal Court ordered the nationwide suspension of X (formerly Twitter) after the company failed to comply with court orders, including requirements concerning a legal representative in Brazil. The Court directed Brazil's telecommunications regulator to implement the suspension.⁵⁰

⁴⁶ Chiara Castro, "A dangerous precedent" – The VPN industry reacts to France's order to block illegal streaming sites, TechRadar (May 2025), <https://www.techradar.com/vpn/vpn-privacy-security/a-dangerous-precedent-the-vpn-industry-reacts-to-frances-order-to-block-illegal-streaming-sites>.

⁴⁷ Amélie Blocman, *Blocking of Streaming Sites Illegally Retransmitting Roland-Garros Tennis Matches*, IRIS 2022-7:1/9, European Audiovisual Observatory (2022), <https://merlin.obs.coe.int/article/9539>.

⁴⁸ Chiara Castro, *French Court Backs LFP and Orders Top VPNs to Block Illegal Football Streams*, TechRadar (Dec. 2025), <https://www.techradar.com/vpn/vpn-privacy-security/french-court-backs-lfp-and-orders-top-vpns-to-block-illegal-football-streams>.

⁴⁹ Internet Society, *Policy Brief: Perspectives on Internet Content Blocking*, "Challenges" (2025), <https://www.internetsociety.org/resources/policybriefs/2025/perspectives-on-internet-content-blocking/>.

⁵⁰ Associated Press, *Brazil Starts Blocking Social Media Platform X Amid a Dispute With Elon Musk*, NPR (Aug. 30, 2024), <https://www.npr.org/2024/08/30/nx-s1-5096220/brazil-suspends-x-elon-musk>.

The order also addressed attempts to circumvent the block. Individuals and companies using technological means, specifically including VPNs, to continue accessing X could face fines of R\$50,000 per day. An initial version of the order also directed Apple and Google to prevent access to VPN applications, although that portion was subsequently withdrawn while the penalty for circumventing the X suspension remained.⁵¹

X was eventually permitted to resume operations after complying with the Court's requirements and paying outstanding fines. But the episode prompted a broader domestic debate about whether and under what circumstances VPN use itself should be restricted. Brazilian legislators subsequently introduced proposals addressing VPN protections, and in 2025 a Chamber of Deputies committee approved legislation intended to protect VPN use for accessing blocked platforms while preserving penalties when VPNs are used for criminal activity or to circumvent judicial decisions.⁵² That legislation remains under consideration.

The Brazilian case demonstrates how enforcement can move from a service to the user's potential means of accessing that service. The original dispute concerned X's compliance with Brazilian law, not VPN technology. Yet making the platform suspension effective led directly to potential penalties for individuals using VPNs to circumvent it.



Iran: VPNs as Lifelines During State Censorship

Iran's policies demonstrate the role VPNs can play when access to the global Internet itself is heavily restricted.

Iranian authorities have long blocked or filtered major international websites and social media platforms while developing the country's National Information Network, a domestic network designed to make Iranian users less dependent on the global Internet. During periods of political unrest, authorities have disrupted Internet connectivity and intensified efforts to block VPNs and other circumvention technologies.⁵³

For many Iranians, VPNs consequently serve a purpose beyond ordinary privacy. They provide a means of reaching information, communications platforms, and services that would otherwise be inaccessible. This has also made VPNs a target of government control. In February 2024, Iran's Supreme Council of Cyberspace prohibited the use of unauthorized VPNs and other circumvention tools, while providing exceptions for government-approved access. Independent VPN services have also faced technical blocking intended to make them more difficult to use.⁵⁴

⁵¹ Luisa Martins, *Moraes recua em decisão sobre uso de VPN*, CNN Brasil (Aug. 30, 2024), <https://www.cnnbrasil.com.br/blogs/luisa-martins/politica/moraes-recua-em-decisao-sobre-uso-de-vpn/>.

⁵² Câmara dos Deputados, *Comissão aprova regras para o uso de redes VPN no Brasil* (Aug. 20, 2025), <https://www.camara.leg.br/noticias/1189786-comissao-aprova-regras-para-o-uso-de-redes-vpn-no-brasil/>.

⁵³ Freedom House, *Freedom on the Net 2024: Iran (2024)*, <https://freedomhouse.org/country/iran/freedom-net/2024>.

⁵⁴ *Id.*

The distinction between authorized and unauthorized VPNs is particularly significant. Rather than eliminating VPN technology altogether, Iran has sought greater control over which services people can use. Freedom House has documented the growth of domestic VPN services alongside restrictions on independent tools, raising concerns that users may be pushed toward services more susceptible to government surveillance or control.⁵⁵

The Iranian government's approach to regulation therefore illustrates the other side of the circumvention debate. The same characteristic that leads some governments to view VPNs as obstacles to enforcement can make them important tools for accessing information under restrictive regimes. Regulation of VPNs can consequently affect not only privacy and cybersecurity, but the practical ability of individuals to reach the global Internet.

Russia: Blocking VPNs and Centralizing Internet Control

Similar to the situation in Iran, Russian policy illustrates how VPN restrictions can become part of a broader technical and legal system for controlling access to the Internet.

Since 2017, Russian law has provided for restrictions on VPN services that allow users to access prohibited online content.⁵⁶ Enforcement expanded significantly in subsequent years, particularly following Russia's invasion of Ukraine, as authorities blocked independent media, international news sources, and major platforms including Facebook and Instagram. VPNs became an important means of reaching many of those services, and consequently an increasing target of Roskomnadzor, Russia's Internet and communications regulator.⁵⁷

The Russian government has pursued these restrictions at several layers. Authorities have blocked individual VPN services, pressured app stores—which act as distribution intermediaries for VPN applications—to remove those applications, restricted information explaining how to circumvent Internet blocks, and prohibited advertising for VPN services.⁵⁸ In October 2024, Roskomnadzor reportedly blocked 197 VPN services that allowed users to reach restricted websites.⁵⁹

⁵⁵ *Id.*

⁵⁶ Dechert LLP, *Russia Passes Measures to Restrict the Use of VPNs and Similar Technology* (Aug. 11, 2017), <https://www.dechert.com/knowledge/onpoint/2017/8/russia-passes-measures-to-restrict-the-use-of-vpns-and-similar.html>.

⁵⁷ *Russian Internet Watchdog Blocks Hundreds of VPN Services*, The Barents Observer (Oct. 25, 2024), <https://www.thebarentsobserver.com/news/russian-internet-watchdog-blocks-hundreds-of-vpn-services/419460>.

⁵⁸ Reporters Without Borders, *Kremlin Steps Up Online Censorship in Order to Silence Last Opposition Voices Ahead of Presidential Election* (Mar. 2024), <https://rsf.org/en/kremlin-steps-online-censorship-order-silence-last-opposition-voices-ahead-presidential-election>.

⁵⁹ *Russian Internet Watchdog Blocks Hundreds of VPN Services*, *supra* note 57.

Russia's government has also attempted to interfere with VPNs at the network level. Its Internet filtering infrastructure uses deep packet inspection and other technical measures to identify and restrict traffic, including VPN traffic. Reported blocking has extended to widely used protocols including OpenVPN and WireGuard.⁶⁰ Because these protocols are not exclusive to consumer circumvention services and are also used by businesses and other organizations for secure networking, such measures demonstrate the difficulty of distinguishing among different uses of the same underlying technology at the network layer.

These measures form part of the Russian government's broader effort to increase state control over its domestic Internet infrastructure, including through the country's "Sovereign Internet" framework.⁶¹ The experience in Russia demonstrates how VPN regulation can progress from restrictions on particular services toward intervention in protocols, distribution channels, information about circumvention, and the underlying networks themselves.

What These Cases Show

Taken together, these cases demonstrate that "VPN regulation" can describe very different forms of government intervention. Some measures regulate the business practices of commercial VPN providers. Others impose obligations on VPN providers as Internet intermediaries, restrict who may provide or use VPN services, penalize circumvention, control distribution through app stores, or attempt to identify and block VPN traffic at the network level.

These distinctions can lead to very different results. The consequences of a requirement imposed directly on a commercial provider may be very different from those of a network-level measure affecting VPN protocols or encrypted traffic. Understanding both the policy objective and the technical layer at which governments intervene is therefore essential to evaluating the likely consequences of any proposed VPN regulation.

Part V: Looking Forward

12. Policy Considerations for a Secure Internet

VPN policy requires governments to balance legitimate objectives involving public safety, cybersecurity, privacy, national security, economic interests, and individual rights. No single regulatory model resolves all of these interests. The following principles are intended to help policymakers evaluate proposed interventions while accounting for the broader security and infrastructure on which VPN services depend.

⁶⁰ Roskomsvoboda, *VPN in Russia: From Blocking Services to Blocking Protocols*, https://roskomsvoboda.org/uploads/en_vpn_in_russia_from_blocking_services_to_blocking_protocols.pdf.

⁶¹ Freedom House, *Freedom on the Net 2019: Russia* (2019), <https://freedomhouse.org/country/russia/freedom-net/2019>.

Strengthen Cybersecurity Without Undermining It

VPNs are widely deployed security technologies used by organizations and individuals to protect communications, infrastructure, and sensitive information. Policies affecting them should therefore be evaluated not only for their intended benefits, but also for their potential cybersecurity consequences.

Depending on their design, restrictions may push users toward less secure or less accountable alternatives, disproportionately affect lawful users of identifiable and audited services, or interfere with secure remote access to critical and distributed infrastructure. Requirements that involve collecting additional sensitive data or documents can increase risks of tracking, identity theft following breaches, and phishing.⁶² Sophisticated malicious actors may also retain access to self-operated or custom technologies that are more difficult to regulate.

These consequences are not arguments against regulation. They are reasons to treat cybersecurity as one of the interests any regulatory intervention must protect.

Target the Right Layer

Internet policy is often implemented through intermediaries capable of observing, restricting, or interrupting particular activity. But technical capability alone does not necessarily mean that an intermediary is best positioned to address the underlying harm.

Policymakers should consider where meaningful knowledge and control actually reside and whether an obligation can be directed toward the relevant conduct or service before moving deeper into general-purpose Internet infrastructure. The further an intervention moves from the activity being regulated, the greater the need to consider its effects on unrelated users and services.

Limit Intermediary Responsibility

Questions about VPN regulation are part of a broader debate over the responsibilities of Internet intermediaries. Similar questions increasingly affect Internet service providers, cloud and hosting providers, domain name operators, and other infrastructure providers.

The U.S. Supreme Court's 2026 decision in *Cox Communications v. Sony Music Entertainment* illustrates an important distinction in U.S. copyright law.⁶³ The Court held that continuing to provide a general-purpose Internet service, even with knowledge that some customers may misuse it, is not by itself sufficient to establish contributory copyright infringement. It also distinguished eligibility for the Digital Millennium Copyright Act's safe-harbor protections from the separate question of liability for users' conduct.

⁶² Internet Society, *supra* note 23.

⁶³ *Cox Communications, Inc. v. Sony Music Entertainment*, 607 U.S. ___, No. 24-171 (2026), https://www.supremecourt.gov/opinions/25pdf/24-171_bq7d.pdf.

This broader principle is significant for Internet infrastructure. If providers face liability merely because general-purpose services can be misused, they may have strong incentives to terminate users, restrict access, or intervene preemptively even when they have limited knowledge of the underlying conduct. Obligations should therefore reflect what an intermediary can reasonably know, control, and address.

Evaluate Proportionality and International Coordination

Governments have legitimate responsibilities to investigate crime, protect the public, and enforce the law. Measures affecting VPNs should nevertheless be proportionate to the specific harm being addressed and account for effects on lawful users, cybersecurity, and Internet infrastructure.

Cross-border coordination is particularly important because VPN services may connect users, providers, infrastructure, and services located in several jurisdictions simultaneously. Conflicting national requirements can create operational complexity, limit providers' ability to offer consistent services across jurisdictions, and contribute to fragmentation of the global Internet. The costs to VPN providers for complying with multiple, country-specific requirements could "limit the ability of new players to compete and increase the costs of secure access for users."⁶⁴

International coordination need not require uniform regulation. Governments can instead pursue interoperability, mutual recognition, and greater consistency where possible while preserving legitimate differences among national legal frameworks. Existing work on cross-border data flows, including through the OECD, provides one model for this kind of cooperation.⁶⁵

Further Considerations for Policymakers

This report does not prescribe a single regulatory framework. Instead it suggests several questions policymakers should ask when considering measures affecting VPNs:

- Does the proposal clearly identify the specific harm it seeks to address?
- Is there reliable evidence that the proposed measure can achieve its intended objective?
- Is the obligation directed toward an actor with meaningful knowledge of and control over that harm, taking account of its role in the Internet ecosystem and its technical capabilities?
- Is intervention occurring at the most appropriate layer of the Internet?
- Could the same objective be achieved through a more targeted or less intrusive approach?
- What effects could the measure have on enterprise cybersecurity, critical infrastructure, and other lawful users?

⁶⁴ Internet Society, *supra* note 23.

⁶⁵ OECD, *Data Free Flow with Trust*, <https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html>.

- Could the intervention push users toward less secure, less transparent, or less accountable alternatives?
- Are the anticipated benefits proportionate to those potential consequences?
- Have technical experts, affected infrastructure providers, industry, and civil society been meaningfully consulted?

These questions do not predetermine policy outcomes. They encourage policymakers to understand both the problem being addressed and the technical consequences of the proposed solution.

Considerations for Industry

Industry also has responsibilities. VPN providers and the broader technical community can strengthen trust through secure engineering, clear privacy practices, independent audits, transparency reporting, effective, responsible governance, and meaningful cooperation with legitimate legal processes.

Voluntary initiatives such as the **VPN Trust Initiative (VTI) Trust Seal** can complement these efforts by establishing common expectations around security, privacy, transparency, and accountability. Such frameworks are strongest when they provide meaningful evidence of responsible practices rather than serving simply as marketing credentials.

Looking Ahead

The following conclusion places these policy considerations in the broader conversation about secure Internet infrastructure.

13. Conclusion

Virtual private networks are often described as consumer privacy tools or technologies used by remote workers and travelers. Those descriptions are accurate, but incomplete.

VPNs are part of the Internet's security architecture. They protect enterprise networks, connect infrastructure, enable secure remote access, and help individuals protect communications across networks they do not control. Recognizing that broader role sharpens the policy conversation. VPN regulation is not simply about consumer software or privacy preferences. It can affect technologies deeply integrated into modern cybersecurity and the operation of the Internet.

Individuals and Businesses Deserve Security

Businesses protect sensitive information because security matters. Financial institutions secure customer communications, healthcare providers protect patient information, and organizations safeguard proprietary systems and data. Individuals have equally legitimate

security and privacy interests as they work, travel, communicate, bank, shop, and conduct other ordinary activities online.

VPNs illustrate the overlap between those needs. The same underlying technologies that help organizations secure communications across untrusted networks can help individuals reduce unnecessary exposure as they participate in digital life.

Protecting privacy is not inherently about concealing wrongdoing. It is often simply about maintaining appropriate control over sensitive information.

Good Policy Starts with Understanding Technology

Sound VPN policy must begin with an accurate understanding of the technology being regulated. VPNs are used across consumer services, businesses, governments, cloud environments, and other forms of Internet infrastructure. Measures aimed at one use can have consequences for others, particularly when intervention occurs at the network or infrastructure layer.

Understanding the full technical consequences of proposed regulation requires input from those who build, operate, study, and rely on these systems. VPN providers, Internet infrastructure operators, cybersecurity experts, civil society, and other affected communities should therefore be part of policy development from the beginning.

Doing so can help produce policies that advance legitimate government interests without unnecessarily undermining user privacy, cybersecurity, or Internet infrastructure. The objective should be to ensure that regulation begins with an accurate understanding of what the technology does, where meaningful knowledge and control reside, and what consequences an intervention may create elsewhere.

The Need for a Broader Conversation About Internet Infrastructure

The questions raised by VPNs are not unique to VPNs. Similar debates increasingly surround encryption, cloud computing, hosting, domain name systems, artificial intelligence, digital identity, and other technologies that provide general-purpose capabilities upon which many different users and services depend.

The rapid development and adoption of artificial intelligence make this broader conversation more urgent. As more consequential activities depend on connected systems, strong encryption, secure networking, and trustworthy Internet infrastructure become increasingly important. Policies that weaken these foundations can create vulnerabilities that extend well beyond their immediate targets. Addressing emerging risks should strengthen the infrastructure on which people and organizations depend, rather than compromise the tools that protect it.

Courts, regulators, industry, technical communities, and civil society will continue to shape these debates as both technology and public policy evolve. New regulatory proposals, court decisions, and technical developments will inevitably change the VPN landscape as well.

For that reason, VPNs at Risk should be understood as a living resource. It will evolve as new developments and case studies provide greater insight into how governments can address legitimate policy objectives while preserving the security, resilience, and openness of the Internet.

The challenge is larger than VPNs. It is how to achieve policy objectives without unnecessarily weakening the general-purpose infrastructure and security capabilities on which everyone else depends.