

DNS at Risk:

How Network Blocking and Fragmentation
Undermine the Global Internet



May 2025

PURPOSE:

This report was developed to address the growing use of Internet infrastructure, particularly Domain Name System (DNS) resolvers and Internet Protocol (IP) routing, as tools for content regulation. It is intended as both a technical and policy-based intervention, grounded in the principles of openness, interoperability, and neutrality that have made the Internet a resilient and generative force for decades.

Its objectives are twofold:

1. **To reinforce the principle that Internet infrastructure must remain content-neutral.** DNS resolvers, routing protocols, and related services form the technical foundation of the Internet and were never designed to evaluate or suppress content. Using them to do so introduces serious risks to security, reliability, and global interoperability.
2. **To document how governments around the world are increasingly deploying infrastructure-level blocking mechanisms**—including DNS blocking, IP filtering, and protocol interference—to pursue a range of policy goals, from copyright enforcement to limiting so-called disinformation in the name of national security. These efforts frequently target neutral infrastructure and services that have no technical relationship to the content in question.

We approach this work from the perspective of Internet infrastructure providers—entities tasked with maintaining the integrity and neutrality of the technologies that keep the Internet running. Our concern is not with the legitimacy of any particular policy goal, but with the long-term consequences of using technical systems for non-technical purposes. We have seen again and again that once a blocking system is built for one reason, it is repurposed years later for another. Without clear constraints, these systems drift from narrow enforcement tools into engines of censorship and fragmentation.

This report urges policymakers, regulators, and technical stakeholders to act now: to reject blunt interventions at the infrastructure layer, to prioritize precision and proportionality in enforcement, and to defend the open Internet before it becomes irreversibly fractured.

EXECUTIVE SUMMARY:

The Internet was designed as a decentralized global network, built on interoperability, open standards, and trust. Yet this architecture is increasingly at risk due to a growing wave of technical blocking measures imposed by governments and private actors. DNS-based restrictions, IP-level filtering, protocol interference, and algorithmic takedowns are being used to pursue a range of policy goals, from copyright enforcement, to limiting so-called disinformation in the interest of national security. However, these measures are too often implemented without legal or technical precision, transparency, or accountability, resulting in overblocking, fragmentation, and collateral damage.

DNS and network-level control tools—particularly those that manipulate foundational Internet infrastructure—are difficult to constrain once they are deployed. As this report explains, the same disruptive infrastructure design modifications ordered and deployed to suppress dissent in Russia and Myanmar are now being proposed and adopted in far less extreme regulatory and geopolitical contexts. Countries like Austria and Malaysia show that reversal is possible, but only when policymakers approach infrastructure governance with clarity and restraint. These systems, once in place, become blunt instruments with profound risk—liable to expand in scope, disrupt lawful services, and erode trust in the global Internet.

DNS blocking is often presented as a quick-fix enforcement solution, but as even its strongest advocates readily concede, it is an easily evaded tool of temporary disruption, and fails to address how to remove infringing content at its source. DNS service providers do not host, transmit, or moderate content—they merely facilitate access. Blocking at the resolver level disrupts convenience, not availability. The content remains accessible through direct IP access, alternative resolvers, VPNs, and other tools, even for non-technical users. As such, DNS blocking is an ineffective and often disproportionate response, especially when it introduces collateral damage, weakens user security, and destabilizes lawful services.

This report outlines the systemic threats posed by these measures, illustrated with real-world case studies from countries including Italy, India, Russia, South Korea, France, and others. These examples reveal how even well-intentioned interventions can destabilize Internet infrastructure, disrupt lawful services, and introduce technical inconsistencies that erode interoperability and trust—especially in geopolitically sensitive environments. Government control of DNS infrastructure is becoming one of the most effective mechanisms for digital censorship. By targeting the DNS resolver layer—particularly recursive resolvers, which are responsible for answering user queries—authorities can imperceptibly shape what is visible, accessible, and even knowable online without users being aware of the manipulation that is occurring. These measures often operate outside of judicial oversight or public transparency, undermining what should be a neutral, globally consistent coordination layer—replacing predictability and interoperability with fragmented, brittle systems shaped by blunt policy enforcement regimes.

KEY FINDINGS INCLUDE:

- **Overblocking is widespread**, particularly when DNS or IP-level restrictions are used against shared infrastructure, such as cloud platforms and content delivery networks. In shared environments, a single IP address or domain often supports dozens or even thousands of unrelated services. Blocking these shared assets can instantly disrupt a wide array of lawful websites, Application Programming Interfaces (APIs), and applications.
- **Content-related Internet fragmentation is accelerating**, with some countries introducing national firewalls, alternative DNS roots, or isolated Internet architectures. While governments may seek to enforce domestic content policies, doing so through infrastructure-level measures creates technical inconsistency, degrades global interoperability, and often fails to achieve the desired outcomes. Enforcement should focus on content removal at the source, rather than interfering with the neutral systems that enable global Internet connectivity, delivering, at best, a temporary reduction in visibility without addressing the underlying content.
- **Collateral damage is severe**, with disproportionate impacts on U.S. cloud, Internet infrastructure, and small businesses—undermining revenue, reliability, investment incentives, and market access in a globally connected economy.
- **Policy interventions often fail to meet their goals**, while simultaneously introducing technical risks, network inefficiencies, and business uncertainty. Left unaddressed, these technical measures threaten the long-term structural design and integrity of open Internet architecture, the health of the digital economy, and the survival of fundamental rights. This report provides evidence of those risks through global case studies, showing how blunt, brute-force network-level interventions often fail to meet their policy objectives while causing disproportionate harm.

For infrastructure operators, cloud providers, and DNS service stakeholders, these developments are not just technical anomalies—they represent growing operational risks, mounting compliance uncertainty, and the erosion of trust in global Internet systems. These interventions not only miss their enforcement mark but actively undermine Internet infrastructure itself—disrupting systems designed for speed, reliability, and scale, and introducing fragility into the core technical architecture upon which commerce, communication, and innovation rely.

CONTENTS:

1. Introduction

2. The Strategic Importance of the Public DNS: Control Point or Cornerstone?

3. How Internet Blocking Works, and Why It Backfires

4. The Technical Risks of Overblocking and Fragmentation

5. Global Case Studies: Real-World Evidence of Harm

a. **India:** Complex Requirements for VPN Service Providers

b. **Malaysia:** DNS Redirection Without Transparency or Consultation

c. **Italy:** Legislative Overreach with 'Piracy Shield'

d. **France:** DNS Resolver and VPN Blocking Mandates

e. **Spain:** Court-Ordered IP Blocking Causes Massive Overreach

f. **Austria:** Court Prohibits IP Blocking Due to Collateral Damage

g. **South Korea:** New Mandate Forces CDN Providers to Block Content

h. **Indonesia:** Government's Extensive IP Blocking to Combat Online Gambling

i. **Myanmar:** Internet Blackouts and Targeted Content Suppression Following Military Coup

j. **Russia:** State-Controlled DNS and Infrastructure Used to Silence Dissent

k. **Venezuela:** DNS Spoofing and Phishing Campaign Targeting Humanitarian Volunteers

l. **Portugal:** Court Orders DNS Blocking by Global Providers, Raising Risk of Overreach

m. **United States:** Domain Seizure Causes Massive Collateral Damage

6. What These Cases Teach Us: Infrastructure-Level Blocking Fails to Deliver Effective Enforcement

7. Recommendations for Preserving Internet Integrity

8. Conclusion and a Path Forward

9. Appendix: Framework for Future Reporting on Overblocking and Fragmentation

1. INTRODUCTION

This report examines the technical impacts of Internet blocking practices, drawing on international case studies to highlight the systemic risks they pose to the Internet’s core functions and the global services that depend on them.

Governments around the world are increasingly turning to DNS-based and other infrastructure-level blocking techniques to restrict access to online content. Yet these tools were never designed to assess or remove content—and using them for that purpose rarely achieves the desired outcome. The content typically remains online and accessible through alternative means, even for non-technical users. What these interventions do produce is significant collateral damage: disruption of lawful services, degraded network performance and efficiency, increased security risks, user confusion, and operational costs that scale with complexity.

As this report documents, infrastructure-level enforcement not only fails to eliminate infringing or unlawful content—it also introduces new operational, economic, and geopolitical risks. DNS and IP blocking frequently impact shared infrastructure, adversely affecting neutral services and third-party providers far beyond the intended target.

The result is a system that fails to address the underlying issue while introducing broader technical and policy complications. When neutral Internet infrastructure is repurposed to serve as a mechanism for content enforcement, the outcome is not precision—it is strain on the foundational protocols that enable global scalability, reliability, and trust. These practices threaten to erode the interoperability and neutrality that have defined the Internet’s success for more than four decades.

To clarify the lens through which this report approaches the issue, we define fragmentation in alignment with the framework developed by the Internet Governance Forum’s Policy Network on Internet Fragmentation (PNIF).¹ This framework identifies multiple forms of fragmentation, including content-access fragmentation (what users can see), application-level fragmentation (what services can function), and technical fragmentation (how the infrastructure itself is affected). Throughout this report, we focus primarily on two of these: (1) content-access fragmentation, which occurs when DNS or IP blocking alters what is reachable by end users, and (2) technical fragmentation, which arises when core infrastructure is manipulated, resulting in inconsistent or broken global functionality. By using DNS and IP-level enforcement to implement content policy, governments risk introducing both forms—creating a degraded, inconsistent Internet experience for users and undermining the underlying architecture that enables global connectivity.

¹ IGF “2024 Policy Network on Internet Fragmentation Output report” January 2025
https://intgovforum.org/en/filedepot_download/256/28579

2. THE STRATEGIC IMPORTANCE OF THE PUBLIC DNS: CONTROL POINT OR CORNERSTONE?

At the heart of the Internet’s architecture lies the Domain Name System (DNS)—a foundational protocol that maps human-readable domain names to machine-readable IP addresses.

At a high-level, the DNS system consists of two parts. On one side sit a series of nameservers (Root, TLD, and Authoritative) that together store information mapping domain names to IP addresses; on the other side sit DNS resolvers (also called recursive resolvers), which query the nameservers to answer where a particular website is located. The nameservers are like the telephone book of the Internet listing names and phone numbers, while recursive resolvers are like the phone operator looking up a number that is being requested. While authoritative nameservers are managed and used directly by website operators, recursive resolvers are selected and used by those individuals browsing the Internet.²

As the connective tissue of global digital communication, public DNS enables billions of devices to locate and interact with services and data across borders.

But DNS is more than just infrastructure—it’s increasingly treated as a strategic control point, acknowledged by both operators³ and governance experts.⁴ When governments exert control by blocking DNS infrastructure, especially resolver services, they acquire a powerful lever to shape, surveil, or restrict user access to the open web. This is because blocking at the resolver level is effectively like removing a listing from a phone book. By refusing to return an IP address in response to requests for a particular website, a DNS resolver can make it appear like an entire website has effectively disappeared from the Internet to an individual using that resolver.

² Cloudflare, “Latest Copyright Decision in Germany Rejects Blocking Through Global DNS Resolvers,” The Cloudflare Blog, April 15, 2024. <https://blog.cloudflare.com/latest-copyright-decision-in-germany-rejects-blocking-through-global-dns-resolvers/>

³ Quad9, “The Public Risk of Governments Controlling DNS Providers,” Quad9 Blog, March 24, 2025. <https://quad9.net/news/blog/the-public-risk-of-governments-controlling-dns-providers/>

⁴ Dawson, Christian. “Defending the Core: Why Internet Values Matter More Than Ever.” CircleID, February 28, 2024. <https://circleid.com/posts/defending-the-core-why-internet-values-matter-more-than-ever>

The risk of overreach is exacerbated by the fact that because DNS returns IP addresses for entire domains, blocking through DNS resolvers can only be done at a domain-wide level. So a blocking order seeking to remove a copyrighted image through DNS blocking—especially for a website with many contributors or user-generated content—would result in blocking all content on the entire domain. This means that applying a block through DNS is likely to block access to content that has not been identified by a court as infringing or otherwise problematic, creating significant proportionality implications.

What therefore begins as a narrowly-defined policy objective—addressing copyright enforcement or online harms—often has unintended consequences without reaching its intended goal.

Control of DNS enables:

- **Censorship** by blocking domains that challenge political narratives or host undesired content.
- **Surveillance** through logging of DNS queries, providing insight into user behavior and preferences.
- **Legal overreach** by imposing liability or compliance obligations on neutral DNS operators.
- **Fragmentation** by incentivizing domestic alternatives or closed DNS ecosystems.

DNS infrastructure was not built to serve as a gatekeeper for national policy enforcement. When repurposed in this way, it becomes a blunt instrument—one that can't distinguish between infringing and lawful content and often impacts unrelated services. This report treats DNS not only as a technical protocol, but as a critical layer of global Internet infrastructure—one whose misuse leads directly to service disruption, economic harm, and disproportionate enforcement outcomes. The policy choices being made today will determine whether DNS remains a neutral conduit or becomes a recurring point of collateral damage in content control efforts.

3. HOW INTERNET BLOCKING WORKS, AND WHY IT BACKFIRES

Having outlined the numerous risks of DNS interference, it's important to recognize that DNS-based blocking is just one method within a broader ecosystem of Internet blocking techniques. Governments and private actors increasingly deploy a range of interventions—each with its own technical risks, policy implications, and fundamental limitations.

This section introduces four categories of blocking practices: DNS-based restrictions, IP-level enforcement, infrastructure-driven fragmentation, and AI-driven filtering. **For detailed case studies demonstrating these dynamics in real-world contexts, see Section 5.** Countries listed here in brief are often explored in greater depth in Section 5, which includes full narrative context and detailed citations. For those not covered in case studies later, footnotes are included in this section to provide direct sourcing.

Critically, these blocking measures are often ineffective. Unlike removing content at the source—such as through the hosting provider—network-level blocks only obscure access via specific pathways. The content itself remains online and accessible through other means. A user can simply switch to an alternative resolver, configure their own, or navigate directly via IP address. As Cloudflare observed in a 2023 analysis of global DNS blocking, “much as having an unlisted phone number didn’t prevent a phone number from being found through other channels and called, a block in a resolver doesn’t preclude an Internet user from navigating to a website in a myriad of other ways.”⁵

When individual governments or courts mandate DNS-based blocking, they are intervening at a foundational layer of Internet architecture design. Because multiple services can share a single domain or IP address—especially in cloud environments—blocking often extends far beyond the intended target, causing widespread collateral damage without guaranteeing removal of the offending material.

⁵ Nemeroff, Patrick. “Latest Copyright Decision in Germany Rejects Blocking Through Global DNS Resolvers.” Cloudflare Blog, April 2, 2024. <https://blog.cloudflare.com/latest-copyright-decision-in-germany-rejects-blocking-through-global-dns-resolvers>.

Forms of technical blocking include:

- **DNS-based blocking**—prevents domain name resolution, but can impact entire platforms hosted under the same DNS name (e.g., Google Drive subdomains).
- **IP-based blocking**—shuts down all services operating from a shared IP address, affecting hundreds or even thousands of unrelated domains.
- **Protocol-based blocking**—restricts encrypted connections (like HTTPS or VPNs), which may degrade user security and privacy. It can also prevent SSL/TLS connections for email server authentication. This includes Deep Packet Inspection (DPI)-based and Server Name Indication (SNI)-based blocking efforts.
- **Automated takedown systems**—often deployed via AI or algorithmic enforcement, these can misclassify legal content and rapidly cause widespread service disruptions.

Although these interventions are often framed as necessary for copyright, national security, or other policy reasons, they frequently cause more harm than good—introducing legal ambiguity, technical fragility, and extensive collateral damage including massive user confusion.

The technical issues raised by these forms of blocking are not theoretical—they are unfolding around the world with real consequences, including for US-based companies and providers. They affect users globally and undermine trust in the providers' global brands.

Importantly, the cases that follow reflect a range of government intent and regulatory contexts. In some jurisdictions—like Russia, Iran, and Myanmar—blocking measures are deliberately used to suppress dissent and control political narratives. In others—such as Italy, Spain, Austria, and France—the interventions were introduced to address legitimate regulatory goals like copyright enforcement or child safety, but have produced significant unintended consequences due to blunt technical execution.

This report draws a clear distinction between political censorship and policy enforcement missteps. However, it also demonstrates that *regardless of intent*, infrastructure-level interventions frequently result in overreach, service disruption, and harm to lawful digital ecosystems.

DNS Blocking and Filtering

- **Italy:** The AGCOM regulator enforces DNS and IP-level blocking to combat copyright infringement, but frequently overblocks, impacting cloud services and platforms.
- **Malaysia:** The national regulator has blocked domains for both copyright and political reasons, creating disruptions beyond intended targets.
- **Russia:** Broad DNS filtering has unintentionally affected services like GitHub and restricted encryption protocols used to evade surveillance.
- **United States:** Domain-level seizures have caused sweeping collateral damage, as seen in the 2011 mooo.com incident that mistakenly took down over 84,000 lawful subdomains.

IP-Based Overblocking

- **Spain:** Blocking of cloud provider IP addresses to address sports streaming led to widespread collateral damage.
- **Austria:** IP blocks on shared infrastructure triggered massive overreach, leading regulators to prohibit the practice.
- **Italy:** Private parties can request IP blocks without government oversight, often impacting legitimate services like Google Drive.
- **Brazil:** IP-based enforcement frequently disrupts unrelated domains hosted on shared infrastructure.⁶
- **South Korea:** Restrictions on gambling and pornography also interfere with VPN services and encrypted traffic.
- **Myanmar:** A 2025 law criminalizes unauthorized VPN use and mandates pre-approval, restricting secure access tools.
- **Australia:** Shared hosting environments have resulted in legal content being cut off under copyright enforcement rules.⁷

6

International Intellectual Property Alliance (IIPA), *2024 Special 301 Report: Brazil*, January 30, 2024, p. 108.
<https://www.iipa.org/files/uploads/2024/01/BRAZIL-2024.pdf>

7

Rebecca Giblin, “Website Blocking Injunctions: Australian Update,” *Kluwer Copyright Blog*, June 14, 2018,
<https://copyrightblog.kluweriplaw.com/2018/06/14/website-blocking-injunctions-australian-update/>

Infrastructure-Driven Fragmentation and DNS Root Integrity

- **China:** DNS tampering and DPI redirect users to domestic alternatives, fragmenting visibility within national borders.⁸
- **Russia:** The “Runet” initiative promotes sovereign DNS and routing infrastructure, signalling potential detachment from global coordination.
- **Iran:** Rewrites DNS responses to steer users toward government-approved services, limiting global content access.⁹
- **Pakistan:** Nationwide filtering policies operate at the infrastructure layer and may interfere with cross-border resolution.¹⁰

Automated and AI-Driven Content Filtering

- **France:** Copyright filters deployed under HADOPI frequently misidentify legal content, triggering wrongful takedowns.
- **United Kingdom:** Broad mandates under the Online Safety Act have introduced reliance on automated filtering systems, raising concerns about potential overblocking—particularly where algorithmic enforcement may extend beyond platforms and lack the human oversight or technical precision needed to avoid infrastructure-level collateral damage.¹¹

These categories illustrate the technical nature and operational risks of infrastructure-based blocking. The following sections delve deeper into global case studies, showing how these techniques have played out in practice—and the consequences they’ve introduced for users, services, and infrastructure operators.

⁸ Nguyen Phong Hoang et al., “How Great is the Great Firewall? Measuring China’s DNS Censorship,” *30th USENIX Security Symposium*, August 2021. <https://www.usenix.org/system/files/sec21-hoang.pdf>

⁹ Freedom House, “Freedom on the Net 2024: Iran,” 2024. <https://freedomhouse.org/country/iran/freedom-net/2024>

¹⁰ Hajira Maryam, “What’s happening with the internet in Pakistan?” *Dawn*, September 2024. <https://www.dawn.com/news/1853742>

¹¹ UK Parliament, “Online Safety Act 2023,” October 26, 2023. <https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted>

4. THE TECHNICAL RISKS OF OVERBLOCKING AND FRAGMENTATION

The most concerning consequences of Internet blocking measures are the systematic incidents of overblocking and Internet fragmentation—both of which result in significant collateral damage to lawful services, infrastructure providers, and end users. These risks are not theoretical; they emerge consistently across jurisdictions and use cases, regardless of the stated policy goal.

Overblocking

Overblocking refers to the unintended restriction of lawful content, services, or infrastructure due to poorly designed or overly broad blocking mechanisms. Governments, regulatory bodies, and private entities implement these measures for various reasons, including intellectual property enforcement, national security, and content moderation. However, the technical execution of these blocking strategies often lacks precision, leading to disproportionate disruptions. All of the forms of technical blocking described above in Section 3 commonly lead to overblocking:

- **DNS-Based Blocking**—Blocking access to entire domains at the DNS resolver level affects not only the intended target but also countless unrelated services hosted under the same domain. When public DNS resolvers are compelled to comply with national blocking mandates, the effects can spill beyond borders—disrupting access for users in other countries and undermining global interoperability.
- **IP-Based Blocking**—Blocking an entire IP address can take down multiple services, especially for websites or services using cloud providers or shared hosting environments.
- **Protocol-Based Filtering**—Filtering mechanisms that indiscriminately block encrypted traffic (e.g., TLS blocking, DPI-based blocking, SNI blocking) interfere with legitimate security measures, forcing users toward insecure alternatives.
- **Automated Takedown Systems**—Overly aggressive automated enforcement mechanisms result in false positives that restrict access to legal services without due process.

These measures introduce systemic risks, including service instability, higher operating costs, degradation or destruction of network efficiencies, loss of access to critical infrastructure, and incentives for users to adopt circumvention technologies that may compromise security. These risks are playing out globally, often with devastating consequences for businesses, infrastructure, and end users. Section 5 below documents a range of real-world examples.

Internet Fragmentation

Technical Internet fragmentation occurs when national or regional policies interfere with the architecture and interoperability of the Internet itself, leading to reduced efficiency, reliability, and global reach. This report focuses on fragmentation that results from direct interference with core infrastructure—but recognizes that content policy decisions, when implemented through technical measures, can also fragment the Internet at the infrastructure level.

While governments may pursue content regulation for a range of reasons, these efforts become a source of fragmentation when they rely on infrastructure-level enforcement—such as DNS manipulation, IP blocking, or mandatory routing changes. These actions alter how the global Internet functions, creating barriers to seamless connectivity and undermining the principle of a shared, open network.

Infrastructure-level fragmentation can arise through:

- **Divergent DNS Root Zones**—The creation of alternative DNS root systems that do not align with the globally coordinated root introduces inconsistencies and undermines universal name resolution.
- **Conflicting Standards for Security and Encryption**—Mandates that interfere with or weaken core security protocols (e.g., TLS, Encrypted Client Hello (ECH), DNS over HTTPS (DoH), or DNSSEC) reduce interoperability and compromise global Internet security.

Content-access fragmentation also contributes to this trend when implemented via technical controls. Though rooted in domestic policy choices, these measures fragment the infrastructure in practice by introducing jurisdiction-specific distortions into what should be a globally consistent system:

- **National Firewalls and Content Restrictions**—Blocking or filtering tools aimed at limiting access to specific categories of content disrupt global service availability when enforced through infrastructure-layer techniques like DNS or IP blocking.
- **Mandatory Local Infrastructure Requirements**—Policies requiring data localization or domestic hosting may impose technical barriers that interfere with cross-border routing, reduce redundancy, and create points of failure.

When infrastructure is used to enforce local content access policies, the result is no longer just content regulation—it is fragmentation of the Internet itself. These practices create inconsistent user experiences, distort routing and resolution behavior, and threaten the resilience of global services.

This report advocates for technical consistency and neutrality in core Internet systems, recognizing that any policy—whether aimed at infrastructure or content—that distorts the operation of global protocols poses a risk to the Internet’s integrity.

Unintended Consequences and Collateral Damage

The negative side effects of blocking regimes extend beyond their intended targets, often causing significant harm to neutral infrastructure providers, digital businesses, and end-users. Key unintended consequences include:

- **Security Risks**—Blocking policies that interfere with encrypted communications drive users toward insecure alternatives, exposing them to surveillance, cybercrime, and data breaches.
- **Economic Barriers**—Businesses operating in multiple jurisdictions must navigate an inconsistent patchwork of regulations, increased compliance costs, and stifling of innovation and market growth.
- **Governance Failures and Lack of Accountability**—Blocking measures are often implemented without sufficient transparency, oversight, or clear legal process. This creates governance risks, erodes institutional trust, and can suppress access to lawful services and information without proper recourse.
- **Operational Instability**—Blanket blocking measures risk disrupting essential services such as cloud computing, domain name resolution, and digital authentication mechanisms.¹² Detailed technical analysis shared by the Internet Engineering Task Force (IETF) Internet Architecture Board (IAB) underscores these concerns and highlights the unintended consequences of blocking mechanisms—particularly when applied to global rendezvous services like DNS and IP-based protocols.¹³ This IAB work warns that such interference can cause wide-reaching collateral damage by breaking core technical functions that underpin the Internet, leading to instability for services far beyond the intended enforcement target.
- **Impact on U.S. Businesses and Users**—Infrastructure-level blocking by foreign governments creates serious challenges for U.S. cloud and Internet providers. Whether through DNS manipulation, IP blocking, or protocol interference, these measures prevent users abroad from accessing lawful U.S.-based services, reducing reliability, eroding trust, and ultimately closing markets. Small- and mid-sized companies—particularly in the cloud, SaaS, and e-commerce sectors—are disproportionately affected. These disruptions also undercut the broader U.S. trade agenda by impeding digital exports and setting precedents that harm the global Internet ecosystem.

Instead of implementing indiscriminate blocking measures, governments should pursue policies that promote a secure, resilient, and open Internet. A more effective approach involves international cooperation, transparency, and the development of precise, narrowly targeted enforcement mechanisms.

¹² Security and Stability Advisory Committee (SSAC), SAC127: DNS Blocking Revisited, ICANN, 16 May 2025. <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac127-dns-blocking-revisited-16-05-2025-en.pdf>

¹³ “Technical Considerations for Internet Service Blocking and Filtering,” [RFC 7754](#), March 2016.

5. GLOBAL CASE STUDIES: REAL-WORLD EVIDENCE OF HARM



India: Complex Requirements for VPN Service Providers

Date of Incident: 2022–Present

Blocking Mechanism Used: App store takedowns, intermediary liability, data logging mandates

Intended Target: Consumer VPN services, cloud providers, and intermediaries

Collateral Damage: Mass market exit by U.S. tech companies; increased surveillance risk; stifled market access

Technical Impact: Friction against privacy tools and intermediary infrastructure; undermined interoperability with global Internet services

Sources and Documentation: Indian IT Rules; app store removals (Oct. 2024); provider testimony

India: Complex Requirements for VPN Service Providers

Context:


India has become a challenging environment for global VPN and cloud providers due to a unique and expansive regulatory framework.¹⁴ In 2022, the government imposed aggressive data logging requirements on intermediaries, including VPN services and cloud infrastructure providers—requirements¹⁵ that conflict with global privacy norms and data minimization principles.¹⁵ Criminal penalties for noncompliance created severe legal risk.

In October 2024, Indian authorities escalated enforcement by unilaterally removing 39 apps—many affiliated with VPN or encrypted communication services—from national app stores.¹⁶ This was done without due process, explanation, or an opportunity to respond. The result is a shrinking market for privacy-enhancing technologies and heightened concerns about India’s commitment to an open Internet.

Many U.S. service providers have exited the Indian market altogether,¹⁷ facing an impossible choice between violating their core business and privacy principles or complying with technically unworkable mandates.¹⁸ These policies not only undermine Internet openness, but also restrict access to digital tools that support free expression and security for Indian users.

¹⁴ Manish, Singh, “India widens regulatory grip over tech firms,” TechCrunch, January 3, 2024, <https://techcrunch.com/2024/01/03/india-tech-regulation/>

¹⁵ Indian Computer Emergency Response Team (CERT-In), Directions under Section 70B of the Information Technology Act, 2000, April 28, 2022. <https://www.cert-in.org.in/Directions70B.jsp>

¹⁶ Manish, Singh, “Cloudflare’s VPN App Among Half-Dozen Pulled from Indian App Stores,” TechCrunch, January 2, 2025. <https://techcrunch.com/2025/01/02/cloudflares-vpn-app-among-half-dozen-pulled-from-indian-app-stores/> 

¹⁷ Varsha Bansal, “VPN Providers Flee India as a New Data Law Takes Hold,” WIRED, September 25, 2022, <https://www.wired.com/story/vpn-firms-flee-india-data-collection-law/>.

¹⁸ Malavika Raghavan, “India’s New Intermediary & Digital Media Rules: Expanding the Boundaries of Executive Power in Digital Regulation,” Future of Privacy Forum, June 10, 2021, <https://fpf.org/blog/indias-new-intermediary-digital-media-rules-expanding-the-boundaries-of-executive-power-in-digital-regulation/>. See also: Manish Singh, “India Widens Regulatory Grip Over Tech Firms,” TechCrunch, January 3, 2024, <https://techcrunch.com/2024/01/03/india-tech-regulation/>.

Malaysia: DNS Redirection Without Transparency or Consultation

Date of Incident: 6 September 2024 (policy enacted); 8 September 2024 (rollback)

Blocking Mechanism Used: Mandatory DNS redirection by ISPs

Intended Target: Various categories of online content deemed illegal by the Malaysian Communications and Multimedia Commission (MCMC), including gambling, pornography, copyright infringement, and scams

Collateral Damage: Blocking of Cloudflare 1.1.1.1 and Google 8.8.8.8 DNS resolver services; user access to encrypted DNS disrupted

Technical Impact: Interference with resolver choice and DNS redirection/poisoning; common strategy used for cyber attacks and undermines DNS privacy and global interoperability; chilling effect on U.S. services

Sources and Documentation: MCMC directives; ISP implementation records; public backlash reported via Malaysian tech communities

Malaysia: DNS Redirection Without Transparency or Consultation

Context:

In September 2024, Malaysia's communications regulator (MCMC) quietly implemented a sweeping policy requiring all Internet Service Providers (ISPs) to redirect DNS traffic to government-controlled resolvers. Citing legal authority under the Communications and Multimedia Act 1998, MCMC issued non-public instructions to block access to foreign DNS providers—including Cloudflare's 1.1.1.1 and Google's 8.8.8.8—without disclosing which content or services were being targeted.¹⁹

The decision sparked immediate public backlash, particularly from Malaysian users who rely on these global DNS services for performance, privacy, and security. No landing pages or notices were provided to affected users. The move effectively cut off encrypted DNS traffic (like DNS-over-HTTPS and DNS-over-TLS), reversing years of progress toward secure resolver adoption and denying Malaysians access to neutral global DNS infrastructure.

The DNS redirection mandate created operational chaos for U.S. companies offering DNS and cloud services in Malaysia. While the policy was eventually reversed,²⁰ the episode highlighted the fragility of international Internet services in the face of opaque national regulation—and raised alarms about future recurrence without proper stakeholder engagement.

Despite Malaysia's ambitions to grow its digital economy (targeting 25.5% of GDP by 2025 and attracting \$14.7 billion in U.S. investment in 2024 alone),²¹ such unilateral interventions undermine market confidence and cast doubt on the country's commitment to open Internet principles. American companies including AWS, Microsoft, and Google have major infrastructure investments in the country,²² making this a critical jurisdiction for responsible governance.

¹⁹ Digital Medusa, DNS Resolvers & Enforcement: The Expanding Role of DNS Providers in Content Blocking, April 2025. <https://digitalmedusa.org/wp-content/uploads/2025/04/DNS-Resolvers-2025-Final.pdf>

²⁰ Reuters. "Malaysia Shelves Web Traffic Re-Routing Plan after Censorship Concerns," Reuters, September 8, 2024. <https://www.reuters.com/technology/malaysia-shelves-web-traffic-re-routing-plan-after-censorship-concerns-2024-09-08/>

²¹ Gobind Singh Deo, Digital Economy Set to Outpace 25.5% GDP Target by End 2025, Free Malaysia Today, September 28, 2024. <https://www.freemalaysiatoday.com/category/business/2024/09/28/digital-economy-set-to-outpace-25-5-gdp-target-by-end-2025-says-minister/>

²² Bernama, Malaysia Welcomes Proposed US\$14.7 Billion Investment by US Tech Giants, October 10, 2024. <https://www.bernama.com/en/news.php?id=2350323>



Italy: Legislative Overreach with ‘Piracy Shield’

Date of Incident: February 2024–present

Blocking Mechanism Used: DNS and IP-based blocking; mandatory compliance by ISPs, VPNs, and DNS providers

Intended Target: Websites streaming unauthorized sports broadcasts (Serie A, UEFA, Italian Cup)

Collateral Damage: Cloudflare IPs hosting 42M+ domains; Google Drive subdomain and IP; legitimate VPN and CDN services

Technical Impact: Widespread service outages; DNS resolver interference; exit of VPN providers from market

Sources and Documentation: Italian regulator AGCOM; Cloudflare testimony; documented outages (February and October 2024)

Italy: Legislative Overreach with ‘Piracy Shield’

Context:

In February 2024, Italy introduced the Piracy Shield, a nationwide system designed to rapidly block unauthorized sports streaming. Developed by a startup affiliated with Lega Serie A—the league behind the policy push—Piracy Shield mandates compliance from ISPs, VPN providers, and DNS resolvers, including global services not based in Italy.

Blocking orders are issued by rights holders without judicial oversight and must be enforced within 30 minutes of notification. There is no mechanism for contesting an order or protecting non-infringing services from unintended consequences. Although initially limited to Italian ISPs, the system has since been expanded to require action from global DNS resolvers and VPNs.

The results have been predictably chaotic. A single Cloudflare IP address—supporting over 42 million domains—was blocked under the policy, rendering countless unrelated websites inaccessible for nearly five hours.²³ In October 2024, AGCOM extended enforcement to Google Drive, mistakenly blacklisting the critical subdomain ²⁴drive.usercontent.google.com, which rendered Drive inaccessible nationwide for hours. CDN resources linked to YouTube were also affected, leading to disruptions in video streaming. While the Piracy Shield includes a whitelist mechanism to prevent such incidents, key services from major platforms like Google were not ²⁵adequately protected. Earlier, in February, a Zenlayer CDN IP was also mistakenly blocked, further compounding the pattern of indiscriminate enforcement.

²³ Andy Maxwell, “Piracy Shield Cloudflare Disaster Blocks Countless Sites, Fires Up Opposition,” TorrentFreak, February 26, 2024. <https://torrentfreak.com/piracy-shield-cloudflare-disaster-blocks-countless-sites-fires-up-opposition-240226/>

²⁴ Mike Masnick, “Italy’s ‘Piracy Shield’ Misfires, Blocks Google Drive In Anti-Piracy Blunder,” Techdirt, October 21, 2024. <https://www.techdirt.com/2024/10/21/italys-piracy-shield-misfires-blocks-google-drive-in-anti-piracy-blunder/>

²⁵ Andy Maxwell, “Piracy Shield IPTV Blocks Reportedly Hit Zenlayer CDN’s Innocent Customers,” TorrentFreak, February 15, 2024. <https://torrentfreak.com/piracy-shield-iptv-blocks-reportedly-hit-zenlayer-cdns-innocent-customers-240215/>

Italy: Legislative Overreach with ‘Piracy Shield’

VPN providers, faced with technically unworkable demands and legal ambiguity, have begun withdrawing from the Italian market.²⁶ The system’s²⁷ lack of accountability and rapid expansion beyond its original scope have drawn criticism for undermining Internet infrastructure and creating an environment where content control is privatized and unregulated. Piracy Shield now stands as a cautionary example of how narrowly scoped policy tools can become blunt, technologically reckless instruments—destabilizing legitimate global services and eroding trust.²⁸

²⁶ Advanced Television, “Italy: Piracy Shield Live but Needs Retweaking,” February 19, 2024. <https://www.advanced-television.com/2024/02/19/italy-piracy-shield-live-but-needs-retweaking>

²⁷ Computer & Communications Industry Association (CCIA), “Re: Italian Piracy Shield and Copyright Law Amendments,” January 2025. <https://ccianet.org/wp-content/uploads/2025/01/Italian-Piracy-Shield-and-Copyright-Law-Amendments-.pdf>

²⁸ Piracy Monitor, “Italy: AGCOM Commissioner Protests Agency’s Rationale Defending Piracy Shield Platform,” December 2024. <https://piracymonitor.org/italy-agcom-commissioner-protests-agencys-rationale-defending-piracy-shield-platform/>



France: DNS Resolver and VPN Blocking Mandates

Date of Incident: May 2023 – ongoing

Blocking Mechanism Used: Court-ordered public DNS resolver blocking; proposed VPN blocking

Intended Target: Pirated sports streaming sites; platforms lacking age verification; sites spreading harmful or illegal content

Collateral Damage: DNS resolver services from U.S. providers (Google, Cloudflare, Cisco); risk of VPN provider exit; heightened censorship potential

Technical Impact: Disruption of neutral resolver services; expansion of liability to DNS operators; fragmentation risks from DNS interference

Sources and Documentation: Paris Judicial Court ruling (May 2024); Digital Services Act alignment bills; Canal+ litigation; press reports on DNS enforcement

France: DNS Resolver and VPN Blocking Mandates

Context:

France has progressively expanded its use of network-level blocking to address a range of policy priorities—from copyright enforcement to child protection and online safety. Article L. 333-10 of the French Sports Code enables rights holders to initiate fast-track court proceedings to block unauthorized broadcasts of sporting events. This authority has increasingly been leveraged to target technical infrastructure rather than infringing content directly.


In May 2024, a Paris court granted broadcaster Canal+ a landmark ruling requiring public DNS providers—including Google, Cloudflare, and Cisco—to implement site-blocking measures typically reserved for Internet Service Providers (ISPs).²⁹ The ruling came after French users circumvented ISP blocks via alternative DNS services, prompting legal efforts to close those loopholes. The court’s action marked the first time these U.S.-based DNS resolver services were compelled to comply with national blocking orders in France, expanding the scope of enforcement to services outside direct French jurisdiction. In response, citing legal risk and operational infeasibility, the U.S. company Cisco decided to cease offering its OpenDNS global DNS resolution service within France,³⁰ highlighting the challenges faced by DNS providers under the new legal requirements.³¹

The pressure has not stopped there. In parallel proceedings, Canal+ and the French football league (LFP) successfully petitioned the court to extend similar blocking obligations to VPN providers.³² This escalation marks a significant expansion of national enforcement mandates to tools traditionally used to protect user privacy. This escalation raises concerns about proportionality, due process, and the technical feasibility of enforcing content restrictions at the VPN layer.³³ VPN providers have stated their intent to challenge the ruling,³⁴ and litigation continues.

29

CircleID, “French Court Orders Google, Cloudflare, Cisco to Poison DNS in Anti-Piracy Crackdown,” June 18, 2024.
<https://circleid.com/posts/20240618-french-court-orders-google-cloudflare-cisco-to-poison-dns-in-anti-piracy-crackdown>

30

Andy Maxwell, “OpenDNS Suspends Service in France Due to Canal+ Piracy Blocking Order,” TorrentFreak, June 29, 2024,
<https://torrentfreak.com/opendns-suspends-service-in-france-due-to-canal-piracy-blocking-order-240629/>. 

31

Telecompaper, “OpenDNS Service Stops in France After Canal Plus Legal Victory Against Piracy,” June 28, 2024.
<https://www.telecompaper.com/news/opendns-service-stops-in-france-after-canal-plus-legal-victory-against-piracy-1505192>

32

TorrentFreak, “Rightsholders Target VPN Providers in French Court to Block Piracy,” February 7, 2025.
<https://torrentfreak.com/rightsholders-target-vpn-providers-in-french-court-to-block-piracy-250207/>

33

The Connexion, “VPN Providers May Leave France Under Pressure from Canal+,” March 29, 2025.
<https://www.connexionfrance.com/news/vpn-providers-may-leave-france-under-pressure-from-canal/712471>

34

TorrentFreak, “Major VPN Providers Ordered to Block Pirate Sports Streaming Sites,” 16 May 2025.
<https://torrentfreak.com/major-vpn-providers-ordered-to-block-pirate-sports-streaming-sites-250516/>

France: DNS Resolver and VPN Blocking Mandates

Ongoing Developments:

The French government is currently advancing legislation that would formalize and expand the legal mandate for blocking on intermediary services like CDN and VPN services, building on the precedent set by the DNS ruling.³⁵ A forthcoming digital bill, anticipated in late 2025, seeks to empower ARCOM (France’s media and communications regulator) with broader authority to compel intermediary service providers to block access to blacklisted sites. This legislative effort coincides with ongoing court proceedings initiated by Canal+ and the LFP to impose blocking requirements on intermediary services.

While framed as a proportional response to online harms, France’s approach blurs critical distinctions between content hosts, network infrastructure, and privacy tools. It raises questions about proportionality, due process, and the long-term technical and geopolitical soundness of compelling infrastructure providers—especially neutral DNS resolvers—to act as gatekeepers for national policy enforcement. The cumulative impact risks fragmenting global Internet services and placing disproportionate burdens on U.S. companies.

35

Hogan Lovells, “France Is Ready to Launch DSA Enforcement in 2025,” January 31, 2025.
<https://www.hoganlovells.com/en/publications/france-is-ready-to-launch-dsa-enforcement-in-2025>



Spain: Court-Ordered IP Blocking Causes Massive Overreach

Date of Incident: Court order issued December 2024; blocking implemented February 2025

Blocking Mechanism Used: IP-based blocking of shared cloud infrastructure

Intended Target: Unauthorized sports streaming platforms (via cloud providers)

Collateral Damage: Thousands of unrelated websites hosted on shared IPs; threats to block entire U.S. cloud networks

Technical Impact: Large-scale overblocking; chilling effect on lawful services; no notice to providers or affected parties

Sources and Documentation: Barcelona court order; reports from Spanish ISPs; statements from U.S. cloud providers; Movistar customer reports

Spain: Court-Ordered IP Blocking Causes Massive Outreach

Context:

In December 2024, a Spanish court in Barcelona granted a request by LaLiga (Spain's top professional football league) and a streaming service to block IP addresses associated with certain cloud hosting providers.³⁶ The court's order permitted immediate enforcement without notifying the infrastructure providers, assessing collateral damage, or establishing appeal mechanisms.

In February 2025, enforcement began—blocking Spanish users from accessing thousands of lawful websites hosted on the same shared IPs as the infringing content. These blocks affected small businesses, SaaS applications, e-commerce platforms, and APIs—many run by or reliant on U.S. cloud providers.³⁷

The ruling's implications went further. LaLiga reportedly used the court's authority to pressure U.S. cloud providers, threatening to block entire IP ranges or networks unless they complied with content removal demands. This tactic exposed a worrying precedent: private rights holders using blunt legal tools to strong-arm infrastructure operators outside the intended jurisdiction of the law.³⁸

Ironically, customers of Telefónica-owned Movistar (a Spanish ISP) also reported being blocked from accessing LaLiga's own websites, a consequence of overbroad IP filtering by the very ISP tasked with enforcing the ruling.³⁹

This case epitomizes the dangers of unstructured, imprecise technical enforcement. The blocking may have satisfied a narrow rights-holder goal, but the costs—service instability, user disruption, and damage to cloud trust—were borne by countless others. It highlights the urgent need for due process, technical precision, and oversight in any Internet blocking regime.

³⁶ Commercial Court No. 6 of Barcelona, Judgment upholding IP address blocking for LaLiga content, December 18, 2024. <https://www.laliga.com/en-GB/news/commercial-court-no-6-of-barcelona-upholds-the-judgment-issued-in-favour-of-laliga-and-dismisses-the-annulments-filed-by-cloudflare-and-rootedcon>

³⁷ Proton VPN, LaLiga is blocking the internet in Spain. A VPN can help, March 20, 2025. <https://protonvpn.com/blog/spain-laliga>

³⁸ Broadband TV News, Cloudflare takes legal action over LaLiga's "disproportionate blocking efforts", February 19, 2025. <https://www.broadbandtvnews.com/2025/02/19/cloudflare-takes-legal-action-over-laligas-disproportionate-blocking-efforts/>

³⁹ TorrentFreak, Piracy Crisis: Cloudflare Says LaLiga Knew Dangers, Blocked IP Address Anyway, February 11, 2025. <https://torrentfreak.com/spain-piracy-crisis-cloudflare-says-laliga-knew-danger-blocked-ip-address-anyway-250211/>

Austria: Court Prohibits IP Blocking Due to Collateral Damage

Date of Incident: IP blocking occurred in 2022; regulator ruling in 2023; appeal withdrawn March 2025

Blocking Mechanism Used: Court-ordered IP-based blocking by Austrian ISPs

Intended Target: 14 websites accused of copyright infringement

Collateral Damage: Thousands of lawful domains hosted on 11 Cloudflare IP addresses

Technical Impact: Large-scale overblocking; service outages; violation of net neutrality principles

Sources and Documentation: Austrian Supreme Court filings; Telecom Control Commission (TKK) ruling; ISPA press release (March 2025)

Austria: Court Prohibits IP Blocking Due to Collateral Damage

Context:

In 2022, a coalition of copyright holders in Austria secured a court order requiring local Internet Service Providers to block 11 IP addresses associated with Cloudflare. The aim was to restrict access to just 14 allegedly infringing websites, but these IPs were part of shared infrastructure used by thousands of legitimate domains.⁴⁰ As a result, a vast number of unrelated websites became inaccessible to Austrian users, causing widespread disruption.

There was no opportunity for the affected parties to be notified or to contest the order. The blocking order was enforced rapidly, with users and service providers left scrambling to understand why lawful sites had disappeared.

The incident triggered a formal complaint from ISPs, who escalated the matter to Austria's independent telecoms regulator, the Telecommunications Control Commission (TKK).⁴¹ In 2023, after a detailed investigation, TKK concluded that IP-based blocking was disproportionate and violated both net neutrality regulations and freedom of expression. The decision represented a landmark regulatory stance in favor of infrastructure neutrality and technical restraint.⁴²

⁴⁰ TorrentFreak, "Austrian ISPs 'Had No Choice' But to Block Pirate Sites AND Cloudflare," August 29, 2022. <https://torrentfreak.com/austrian-isps-had-no-choice-but-to-block-pirate-sites-and-cloudflare-220829/>

⁴¹ Cullen International, "Austrian Telecoms Regulator Decides Against Blocking of IP Addresses," September 8, 2023. <https://www.cullen-international.com/news/2023/09/Austrian-telecoms-regulator-decides-against-blocking-of-ip-addresses.html>

⁴² Matthias Leistner, "Copyright Based IP-Blocks of Structurally Infringing Websites vs. Net Neutrality: Has the Austrian Telecom Regulator Got It Right?" SSRN, October 13, 2024. <https://ssrn.com/abstract=4986403>

Austria: Court Prohibits IP Blocking Due to Collateral Damage

In a major development in March 2025, the rights holders withdrew their appeal of the TKK decision, shortly after the case was referred to the European Court of Justice (ECJ). This made the TKK's ruling final and binding, setting a national precedent that reinforces legal limits on indiscriminate technical enforcement.

For U.S. cloud providers like Cloudflare—and the many American businesses whose websites are hosted on shared IP infrastructure—this case was a significant win.⁴³ It affirmed the principle that shared infrastructure cannot be treated as collateral damage in narrow enforcement efforts, and that governments must apply proportionality and precision when regulating the Internet.⁴⁴

The Austrian case is now a model for other European regulators, offering a clear example of how net neutrality and human rights frameworks can be applied to check technical overreach.

⁴³ Matthew Prince, “Thoughtful decision by Austrian authorities. Governments have the right to limit some content on the networks within their borders, but doing so at the IP level causes too much collateral damage. DNS-based blocking is more precise and less disruptive.” X (formerly Twitter), August 19, 2023.
<https://twitter.com/eastdakota/status/1692739316307386451>

⁴⁴ RTR, “Net Neutrality Report 2024,” August 2024.
https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/netzneutralitaetsbericht/RTR_Net_Neutrality_Report-2024.pdf

South Korea: New Mandate Forces CDN Providers to Block Content

Date of Incident: Law amended December 2023; enforcement began July 2024

Blocking Mechanism Used: Mandatory content blocking by CDN providers

Intended Target: Broad categories of illegal content under South Korean law (gambling, pornography, defamation, etc.)

Collateral Damage: Redundant blocking across multiple layers of infrastructure; compliance burdens on non-hosting providers

Technical Impact: Operational inefficiencies, legal uncertainty, potential service withdrawal from market

Sources and Documentation: Korean Network Act (2023 revision); industry feedback; provider compliance guidance; market forecasts

South Korea: New Mandate Forces CDN Providers to Block Content

Context:

In December 2023, the South Korean legislature amended its Network Act to create a world-first mandate: content delivery network (CDN) providers are now required to block access to content that South Korean authorities have deemed illegal.⁴⁵ This obligation went into effect in July 2024, adding a new layer of enforcement to a country already known for one of the most aggressive Internet filtering regimes in the world.

South Korea's largest ISPs already implement widespread blocking, with over 100,000 content blocks reportedly approved each year.⁴⁶ However, this new mandate extended that responsibility to CDN providers, who—critically—do not host the content themselves. CDN services cache and distribute content to optimize speed and reduce latency, but lack visibility or control over the actual data being served.

This legal shift forced global CDN companies—many of them U.S.-based—to implement redundant and costly compliance systems. For example, if a South Korean regulator designates a video stream or website as illegal, both the ISP and the CDN must now block it, even if the CDN has no direct relationship with the source content or platform. The regulation introduces technical confusion and legal risk, especially for companies that serve content from outside South Korea but deliver it locally via global networks. With no clear standards for determining illegality, and no hosting control, CDNs are left in an untenable position—liable for content they didn't publish, can't remove, and may not even know they are serving.

⁴⁵ Joonhyuk Kim, "Bill Introduced to Block Access to Nunu TV at the Source," Financial News (Fnnews), March 22, 2023, <https://www.fnnews.com/news/202303221823424151>.

⁴⁶ Freedom House. (2023). South Korea: Freedom on the Net 2023. Retrieved from <https://freedomhouse.org/country/south-korea/freedom-net/2023>

South Korea: New Mandate Forces CDN Providers to Block Content

47

As South Korea's CDN market is expected to reach \$3.8 billion by 2030, the law raises serious barriers to U.S. participation. It is likely to push smaller providers out entirely, and could force larger companies to reevaluate investment in South Korean infrastructure. Although not the primary focus of the 2023 Network Act amendments, South Korea's enforcement environment has long included aggressive restrictions on VPN services—creating a broader ecosystem in which encrypted access tools face scrutiny alongside CDN operators.

This case is emblematic of a broader trend: governments pushing enforcement duties further “down the stack” onto infrastructure operators not equipped—or appropriate—for content adjudication. Without multistakeholder governance and clearer international norms, countries may continue adopting fractured, burdensome regimes that risk breaking the Internet's global reach.

⁴⁷ Grand View Research. “South Korea Content Delivery Network Market Size & Outlook, 2030.” Horizon, 2024.
<https://www.grandviewresearch.com/horizon/outlook/content-delivery-network-market/south-korea>



Indonesia: Government's Extensive IP Blocking to Combat Online Gambling

Date of Incident: October 2024 to January 2025

Blocking Mechanism Used: IP-based blocking

Intended Target: Online gambling websites

Collateral Damage: Potential disruption of legitimate websites sharing the same IP addresses

Technical Impact: Risk of overblocking due to shared IP addresses among multiple domains

Sources and Documentation: Indonesian Ministry of Communication (Komdigi) statements (2024–2025); Gambling Insider reporting; U.S. Small Business Administration small business data (2023)

Indonesia: Government's Extensive IP Blocking to Combat Online Gambling

Context:

Between October 2024 and January 2025, Indonesia's Ministry of Communication and Digital Affairs (Komdigi) intensified its crackdown on online gambling, blocking over 700,000 pieces of related digital content across various platforms.⁴⁸ This initiative aimed to protect the public, especially youth, from the adverse effects of online gambling.⁴⁹

However, the implementation of IP-based blocking raised significant concerns. In today's Internet architecture, multiple domains often share a single IP address, especially when hosted on shared or cloud-based servers.⁵⁰ Consequently, blocking an IP address associated with a gambling site inadvertently restricted access to numerous unrelated, legitimate websites. This overblocking disrupted businesses and impeded users seeking non-gambling content.

⁴⁸ Gambling Insider, "Indonesia Blocks Over 43,000 Online Gambling Advertisements in Early 2025," Gambling Insider, January 15, 2025, <https://www.gamblinginsider.com/news/27922/indonesia-blocks-over-43000-online-gambling-advertisements-in-early-2025>.

⁴⁹ Digital Policy Alert, "Indonesia: Ministry of Communication and Information Policy on Content Moderation Enforcement Regarding Online Gambling," Digital Policy Alert, January 6, 2025, <https://digitalpolicyalert.org/change/6719-kominfo-content-moderation-enforcement-regarding-online-gambling>.

⁵⁰ Cloudflare, "The Unintended Consequences of Blocking IP Addresses," Cloudflare Blog, August 11, 2022, <https://blog.cloudflare.com/consequences-of-ip-blocking>.

Indonesia: Government's Extensive IP Blocking to Combat Online Gambling

The economic implications were particularly pronounced for U.S. small businesses. According to the U.S. Small Business Administration (SBA), small businesses comprise 99.9% of all U.S. firms and employ 46.4% of private sector employees.⁵¹ Many of these businesses rely on global Internet infrastructure to reach international markets. Trade presents a tremendous opportunity for small U.S. businesses to grow, with nearly 96% of the world's consumers living outside U.S. borders.⁵² Indonesia's overblocking poses barriers to market entry and continuity, affecting the growth and sustainability of these enterprises.

This incident underscores the need for governments to adopt precise and transparent methods when regulating online content. While the intent to curb online gambling may be valid, the approach must ensure minimal disruption to lawful online activities. Collaborative efforts involving international stakeholders, clear guidelines, and the adoption of advanced technologies can help achieve policy objectives without compromising the integrity and accessibility of the global Internet.

⁵¹ U.S. Small Business Administration, Office of Advocacy. "Frequently Asked Questions About Small Business, 2023." March 7, 2023. <https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/>.

⁵² U.S. Small Business Administration. "Export Products." SBA.gov, October 31, 2024. <https://www.sba.gov/business-guide/grow-your-business/export-products>.



Myanmar: Internet Blackouts and Targeted Content Suppression Following Military Coup

Date of Incident: February 2021 (military coup) through 2025 (ongoing restrictions)

Blocking Mechanism Used: Nationwide Internet shutdowns; DNS and IP blocking; VPN restrictions

Intended Target: Political dissent, independent journalism, opposition movements, and circumvention tools

Collateral Damage: Disruption to all digital services including e-commerce, communication platforms, and humanitarian coordination tools

Technical Impact: Widespread Internet unavailability; forced reliance on risky circumvention tools; surveillance and malware exposure

Sources and Documentation: Myanmar Cybersecurity Law (2025); AP, Reuters, VietnamPlus reporting; regional civil society monitoring

Myanmar: Internet Blackouts and Targeted Content Suppression Following Military Coup

Context:

Since Myanmar's February 2021 military coup, the ruling junta has used technical blocking and Internet shutdowns as central tools for censorship and control. In the coup's immediate aftermath, Myanmar imposed nationwide Internet blackouts to suppress resistance and disrupt organizing efforts. These later evolved into targeted, region-specific shutdowns and restrictions on circumvention tools like VPNs.

In 2025, the junta formalized its approach through the Cybersecurity Law No. 1/2025, which criminalizes unauthorized online gambling, fraud, and speech deemed threatening to national security.⁵³ However, the law also criminalizes unauthorized VPN provision and provides sweeping authority to surveil, block, and penalize online content and services, with vague provisions and no judicial safeguards.⁵⁴

⁵³

Associated Press, "Myanmar's military rulers enact cybersecurity law with wide-ranging censorship provisions," January 3, 2025. <https://apnews.com/article/8128ba7a2c02555217c6a64ab641eaf6>

⁵⁴

Radio Free Asia, "Myanmar enacts cybersecurity law that aims to restrict use of VPNs," January 2, 2025. <https://www.rfa.org/english/myanmar/2025/01/02/cybersecurity-law-vpn/>

Myanmar: Internet Blackouts and Targeted Content Suppression Following Military Coup

These policies have had devastating effects on Myanmar’s digital ecosystem. Thousands of small businesses, many of which operate through platforms like Facebook, have gone offline—either because their platforms were blocked or out of fear of reprisal. Reports from regions like Bhamo detail a spike in illegal gambling dens and crime, while foreign nationals have been detained in anti-fraud sweeps targeting alleged online operations.

Access to the global Internet in Myanmar is now mediated by an opaque mix of government orders, ISP-level censorship, and DNS manipulation.⁵⁵ Attempts to use VPNs are increasingly met with malware risks, phishing attacks, and potential arrest.⁵⁶

For U.S. businesses, particularly digital platforms and service providers, Myanmar’s environment is essentially non-operational. The political instability, combined with technical unreliability and legal risk, makes service provision untenable. And for global human rights and connectivity advocates, the Myanmar case represents one of the clearest examples of how DNS and network control can become instruments of repression.

⁵⁵ Voice of America, “Report: In record year of internet shutdowns, Myanmar leads,” February 24, 2025.
<https://www.voanews.com/a/report-in-record-year-of-internet-shutdowns-myanmar-leads/7985585.html>

⁵⁶ Surachanee Sriyai, “Myanmar Junta’s Internet Controls Expose Citizens to More Cyber Threats,” Fulcrum, August 5, 2024,
<https://fulcrum.sg/myanmar-juntas-internet-controls-expose-citizens-to-more-cyber-threats/>.

Russia: State-Controlled DNS and Infrastructure Used to Silence Dissent

Date of Incident: 2019 (technical infrastructure mandates) through 2025 (escalating censorship and blocking)

Blocking Mechanism Used: DNS manipulation, IP and protocol blocking, DPI, forced domestic routing, VPN bans

Intended Target: Foreign platforms, political dissent, independent journalism, social media, privacy tools

Collateral Damage: Service outages affecting neutral infrastructure; degraded access to global platforms; chilling effect on civil society and free expression

Technical Impact: Network instability, traffic isolation, forced use of state-controlled DNS, increased surveillance and fragmentation

Sources and Documentation: Russian Sovereign Internet Law; Roskomnadzor directives; AP, Reuters, OONI reporting; operator testimony

Russia: State-Controlled DNS and Infrastructure Used to Silence Dissent

Context:

Russia has become a global exemplar of how national governments can weaponize DNS control and infrastructure mandates to assert information dominance. Since 2019, its Internet regulator, Roskomnadzor, has deployed a nationwide censorship regime rooted in technical manipulation, including the installation of black-box surveillance and filtering devices at ISPs under the so-called *Sovereign Internet Law*.⁵⁷

These “black boxes” enable deep packet inspection (DPI), protocol blocking, and forced DNS redirection—all without user consent or oversight.⁵⁸ Russia has also developed an alternative DNS root system, and mandated that traffic remain within national borders, creating a fragmented and monitored digital environment.

This architecture has been used to enforce widespread content restrictions. Platforms like Facebook, YouTube, Twitter, LinkedIn, Instagram, and sites such as the BBC have all been blocked or throttled. GitHub and other neutral services have faced temporary outages due to their role in hosting politically sensitive content. Russian authorities also routinely attempt to block VPNs, closing off paths to the global Internet.⁵⁹

⁵⁷ Internet Society, Russia’s ‘Sovereign Internet’ Law, November 2019. <https://www.internetsociety.org/resources/internet-fragmentation/russias-sovereign-internet-law/>

⁵⁸ The Moscow Times, Russia’s Sovereign Internet Law Comes Into Force, November 1, 2019. <https://www.themoscowtimes.com/2019/11/01/russias-sovereign-internet-law-comes-into-force-a68002>

⁵⁹ TechRadar, Russia Demands Over 200 VPNs Are Removed from the Play Store, April 2025. <https://www.techradar.com/vpn/vpn-privacy-security/russia-demands-212-vpns-are-removed-from-the-play-store-but-google-is-resisting>


Russia: State-Controlled DNS and Infrastructure Used to Silence Dissent

For U.S. technology companies, the Russian market has become effectively unreachable. Compliance would require enabling censorship and surveillance, while non-compliance leads to service degradation or outright blocking. Even neutral infrastructure providers, like DNS and cloud services, have been caught in the crossfire—facing service outages, legal threats, and loss of user base.⁶⁰

The global concern is not just Russia's actions alone, but the exportability of this model. Countries like India, Myanmar, and Ethiopia are reportedly emulating aspects of Russia's infrastructure control regime. As geopolitical tensions mount, the Russian example highlights how DNS and network fragmentation can be deployed not just for domestic control, but as a blueprint for information sovereignty around the world.⁶¹

⁶⁰ OONI, The Systematic Suppression of Independent Media in Russia, November 2024. <https://ooni.org/post/2024-russia-report/>

⁶¹ Carnegie Endowment for International Peace, Throttling of YouTube Shows That Russia Is Getting Better at Online Censorship, February 2025. <https://carnegieendowment.org/russia-eurasia/politika/2025/02/russia-youtube-block-attempt>



Venezuela: DNS Spoofing and Phishing Campaign Targeting Humanitarian Volunteers

Date of Incident: February–March 2019

Blocking Mechanism Used: DNS spoofing and injection by local ISPs

Intended Target: Opposition-led humanitarian aid initiative and civil society volunteers

Collateral Damage: Exposure of private user data; erosion of DNS trust; suppression of civil society organizing

Technical Impact: Government-created phishing domain redirected users from legitimate site; DNS integrity compromised; surveillance enabled through credential harvesting

Sources and Documentation: VE sin Filtro technical report (2019); OONI/VE sin Filtro presentation (2020); civil society testimony

Venezuela: DNS Spoofing and Phishing Campaign Targeting Humanitarian Volunteers

Context:

Amid Venezuela's deepening humanitarian crisis in early 2019, opposition leader Juan Guaidó launched a public call for volunteers to assist in the distribution of international aid. Civil society groups and volunteers were encouraged to register via a secure website, *voluntariosxvenezuela.com*. In response, the Venezuelan government orchestrated a targeted DNS manipulation campaign to undermine the effort and gather intelligence on participants.⁶²

According to technical documentation from Venezuelan digital rights group VE sin Filtro and corroborated by the Open Observatory of Network Interference (OONI), multiple state-aligned Internet Service Providers (ISPs) engaged in DNS spoofing and injection.⁶³ When users attempted to visit the legitimate volunteer site, their DNS queries were intercepted and redirected to a nearly identical phishing domain—*voluntariosvenezuela.com*—controlled by the state. This fake site harvested names, phone numbers, and other personal details of individuals attempting to sign up to help.

The phishing campaign was made possible through DNS poisoning at the resolver level—a tactic that undermined fundamental trust in the DNS system.⁶⁴ Affected users had no clear indication that they were being redirected, and no warnings were provided by ISPs or the government. The goal was not only to deter civic participation but to identify and surveil political dissenters under the guise of national security.⁶⁵

⁶² VE sin Filtro, “Phishing by Venezuelan Government Puts Activists and Internet Users at Risk,” VE sin Filtro, February 12, 2019, https://vesinfiltro.com/noticias/Phishing_by_Venezuelan_government_targets_activists/.

⁶³ Andrés Azpúrua and Carlos Guerra, “Phishing by Venezuelan Government Puts Activists and Internet Users at Risk,” VE sin Filtro, February 15, 2019, https://vesinfiltro.com/noticias/Phishing_by_Venezuelan_government_targets_activists/. Also Maria Xynou, “Measuring Internet Censorship,” presented at Internet Measurement Village 2020, June 10, 2020, Open Observatory of Network Interference (OONI), <https://ooni.org/documents/imv2020-slides/ooni.pdf>.

⁶⁴ Kaspersky Lab, “DNS Manipulation in Venezuela in Regards to the Humanitarian Aid Campaign,” Securelist, February 13, 2019, <https://securelist.com/dns-manipulation-in-venezuela/89592/>.

⁶⁵ Freedom House, “Venezuela: Freedom on the Net 2019 Country Report,” Freedom House, 2019, <https://freedomhouse.org/country/venezuela/freedom-net/2019>.

Venezuela: DNS Spoofing and Phishing Campaign Targeting Humanitarian Volunteers

Context:

This incident stands as a stark example of DNS abuse as a tool of repression. Unlike conventional blocking, DNS manipulation in this case served an active offensive purpose: to deceive, surveil, and compromise users who were acting in good faith.⁶⁶ It also revealed the role that ISPs can play in implementing government-aligned censorship and surveillance at scale.

The Venezuelan case illustrates a critical risk: when DNS infrastructure is weaponized, it becomes not only a vector for censorship, but a tool for entrapment—turning Internet architecture into a mechanism for state control.

⁶⁶ VE sin Filtro, “Internet Censorship, DNS Poisoning and Phishing in Venezuela,” Presentation Slides, 2020, <https://ooni.org/documents/imv2020-slides/vesinfiltro.pdf>.



Portugal: Court Orders DNS Blocking by Global Providers, Raising Risk of Overreach

Date of Incident: September 2024 – ongoing (under appeal)

Blocking Mechanism Used: Court-ordered DNS blocking by global DNS providers

Intended Target: Allegedly infringing streaming and torrent websites

Collateral Damage: Chilling effect on DNS service availability in Portugal; threat to lawful platforms operating under same domain structures; increased risk of service withdrawal

Technical Impact: Potential overblocking via domain-wide DNS filtering; legal uncertainty for resolver operators; erosion of resolver neutrality

Sources and Documentation: Portugal News reporting (2024); Shine Business coverage (2024); Cisco and OpenDNS provider statements (2024); industry press reporting on resolver withdrawal

Portugal: Court Orders DNS Blocking by Global Providers, Raising Risk of Overreach

Context:

In September 2024, the Lisbon Intellectual Property Court ordered Google Portugal to block access to the domain and more than 500 subdomains of the website EZTV, accused of facilitating unauthorized sharing of films, series, and other content.⁶⁷ The court imposed a fine of €1,000 for each day of non-compliance after the ruling became final. Google Portugal has appealed the decision, arguing that DNS resolution is operated by Google Ireland, and that DNS blocking does not remove infringing content, but merely obscures access—raising fundamental questions of jurisdiction and efficacy.⁶⁸

The ruling is part of a broader trend across Europe, where national courts are extending enforcement obligations to neutral DNS service providers—including Cloudflare and Cisco.⁶⁹ In response to similar legal pressure in both Portugal and France, Cisco discontinued OpenDNS services, citing growing legal uncertainty and the technical risks of mandated filtering. These actions highlight the chilling effect such rulings can have on the global availability of essential infrastructure services.

⁶⁷ “Google Portugal Ordered to Block Pirate Site,” The Portugal News, September 18, 2024, <https://www.theportugalnews.com/news/2024-09-18/google-portugal-ordered-to-block-pirate-site/92193>.

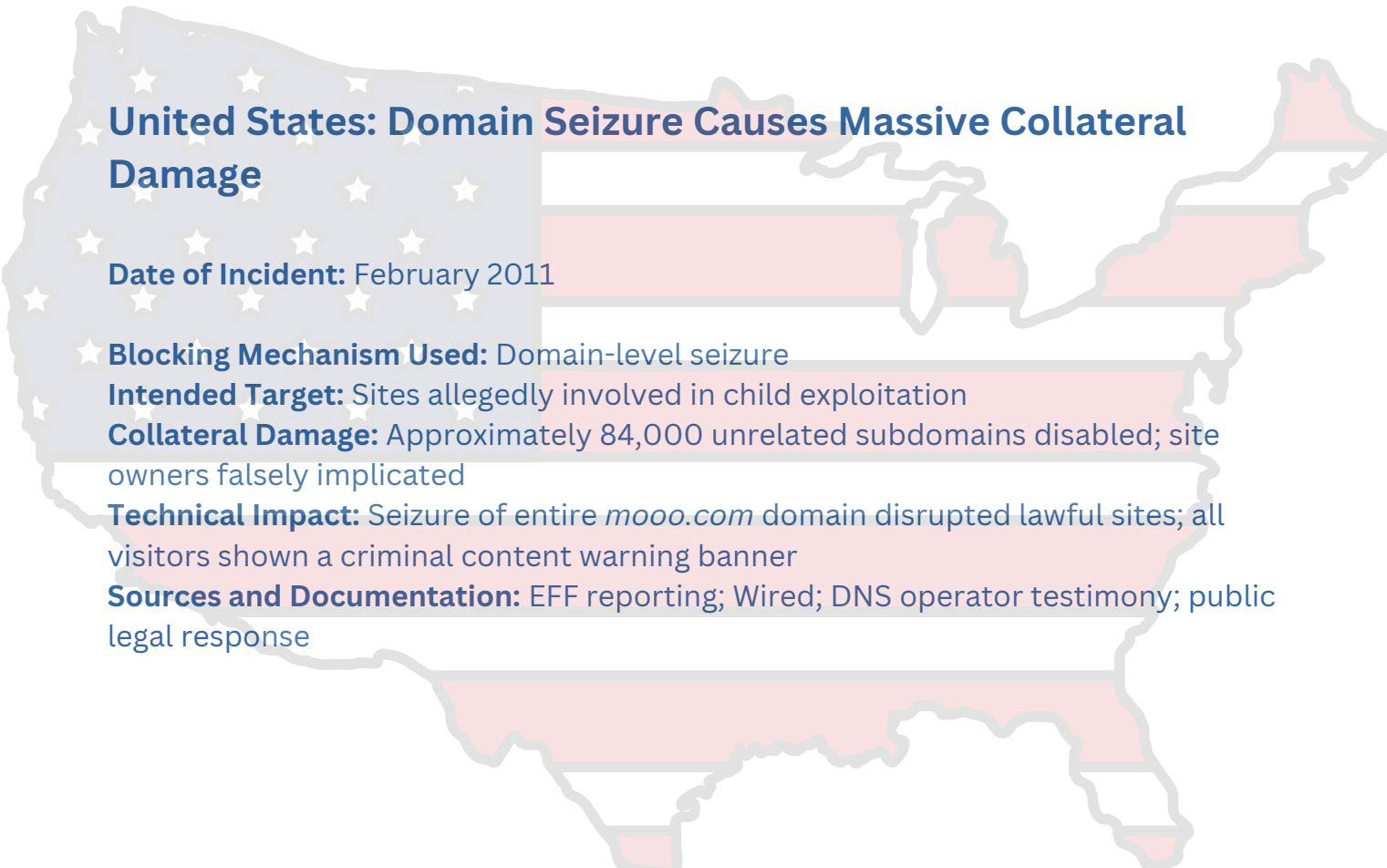
⁶⁸ “Google Portugal to Appeal Court Order to Block Pirate Site,” Shine, September 20, 2024, <https://www.shine.cn/biz/company/2409186481/>.

⁶⁹ “Cisco Pulls OpenDNS from France and Portugal After Court Orders Blocking,” Broadband TV News, July 2, 2024, <https://www.broadbandtvnews.com/2024/07/02/cisco-pulls-opendns-after-canal-plus-order/>. Also “OpenDNS Pulls Plug on France and Portugal After Web Blocking Injunctions Targeting Football Piracy,” Complete Music Update, July 2, 2024, <https://completemusicupdate.com/opendns-pulls-plug-on-france-and-portugal-after-web-blocking-injunctions-targeting-football-piracy/>.

Portugal: Court Orders DNS Blocking by Global Providers, Raising Risk of Overreach

Like other DNS-based blocking mandates, the Portuguese order compels non-hosting infrastructure providers to make content determinations they are neither equipped nor authorized to make. It raises the likelihood of overblocking lawful services that share domain infrastructure—particularly platforms with user-generated content or those hosted via CDNs.

What makes the Portugal case especially troubling is that it demonstrates how a single national decision—issued unilaterally and without consultation with technical experts, civil society, or global Internet governance bodies—can force global infrastructure providers to implement country-specific censorship, even at the expense of lawful content or foreign users. In effect, it allows one jurisdiction’s courts to shape the visibility of online content worldwide by compelling action at the infrastructure layer. The result is a dangerous precedent: infrastructure designed to serve everyone equally becomes fragmented by localized demands, eroding global consistency and trust in the Internet’s foundational systems.



United States: Domain Seizure Causes Massive Collateral Damage

Date of Incident: February 2011

★ **Blocking Mechanism Used:** Domain-level seizure

Intended Target: Sites allegedly involved in child exploitation

Collateral Damage: Approximately 84,000 unrelated subdomains disabled; site owners falsely implicated

Technical Impact: Seizure of entire *mooo.com* domain disrupted lawful sites; all visitors shown a criminal content warning banner

Sources and Documentation: EFF reporting; Wired; DNS operator testimony; public legal response

United States: Domain Seizure Causes Massive Collateral Damage

Context:

In February 2011, the U.S. Department of Homeland Security, under “Operation Protect Our Children,” mistakenly seized the domain mooo.com as part of a law enforcement effort targeting child exploitation. The domain, operated by FreeDNS, hosted more than 84,000 subdomains—many of which belonged to lawful personal, nonprofit, and small business websites.⁷⁰

For nearly two days, all traffic to these unrelated sites was redirected to a Department of Justice banner falsely stating that the site had been seized for hosting child sexual abuse material (CSAM). The reputational damage to site owners was severe, and public outcry forced the domain’s rapid restoration.

The incident became one of the earliest and most striking examples of the dangers of imprecise technical enforcement. It demonstrated how government-led infrastructure actions—absent clear safeguards and technical understanding—can cause sweeping harm to lawful Internet services and users.

70

David Kravets, “DHS Seizes Domain Names, Redirects to Anti-Child Porn Message,” Wired, February 16, 2011, <https://www.wired.com/2011/02/dhs-seizes-domain-names/>; Also “EFF Urges ICE to Exercise Caution When Seizing Domains,” Electronic Frontier Foundation, February 21, 2011, <https://www.eff.org/press/releases/eff-urges-ice-exercise-caution-when-seizing-domains>

6. WHAT THESE CASES TEACH US: INFRASTRUCTURE-LEVEL BLOCKING FAILS TO DELIVER EFFECTIVE ENFORCEMENT

The following section synthesizes the lessons from our global case studies—distilling common patterns and policy failures that emerge when governments deploy DNS and other network-level blocking tools. Together, they show a dangerous drift toward censorship-by-infrastructure.

When governments implement DNS manipulation or IP blocking for example, the results follow a pattern—whether the intent is anti-piracy, political censorship, or public safety. As the case studies in this report demonstrate, once the infrastructure for network-level control is built, it becomes trivially easy to repurpose for other aims. The same DNS and IP-blocking capabilities used by authoritarian regimes in Russia and Myanmar to suppress dissent are also being deployed—often under legal pretext—in democratic countries like Italy, France, and Spain.

But not all outcomes are equal. Some countries are beginning to course-correct. Austria has ruled IP-level blocking incompatible with net neutrality. Malaysia quickly reversed its DNS redirection policy following public backlash. These examples show that better choices are possible—and that policy errors can be reversed.

The key lesson from these case studies is clear: infrastructure-level blocking is an imprecise enforcement strategy that creates outsized harm relative to its intended purpose. Even when deployed with the best intentions—such as combating piracy or protecting users—these measures frequently result in overreach, service disruption, and liability exposure for neutral providers. Technical enforcement should be approached with precision, restraint, and accountability. Without such safeguards, narrowly scoped content restrictions can lead to broad, unintended consequences that harm lawful services and destabilize critical Internet infrastructure.

7. RECOMMENDATIONS FOR PRESERVING INTERNET INTEGRITY

To ensure the continued stability and resilience of the Internet, policymakers, regulators, and infrastructure operators should adhere to the following principles:

- 1. Do Not Use Network-Level Blocking**—Policies that mandate blocking at the DNS resolver, IP, or protocol level should be firmly rejected. These blunt tools compromise critical Internet infrastructure—recursive resolvers, shared cloud IPs, encryption protocols—by turning them into enforcement mechanisms for content policy. Such infrastructure was built for scale, speed, and security—not censorship. When neutral systems are forced to block content, the result is not precision enforcement, but systemic risk: overblocking, service outages, user confusion, and fragmentation of the global Internet. Shared technical resources that power lawful commerce, security tools, and communication platforms should not be collateral damage in content disputes.
- 2. Target Content at the Source**—Effective enforcement starts with precision. Rather than disrupt neutral infrastructure, policymakers and rights holders should work to remove illegal content at its origin—through hosting providers, platforms, or via international cooperation with local authorities. A recent example is the 2024 shutdown of Fmovies, achieved through targeted legal and government action in Vietnam—not by breaking DNS or IP routing.⁷¹ This collaborative, source-level approach succeeded where blocking fails: it removed the content entirely without destabilizing global infrastructure or harming lawful services. Content enforcement must focus on the actors responsible, not the infrastructure that delivers the modern Internet.
- 3. Require Transparency and Due Process**—Blocking mechanisms must be subject to independent oversight, clear public justification, and avenues for appeal.

71

World's largest' piracy ring Fmovies shut down by police in Vietnam," The Guardian, August 29, 2024.
<https://www.theguardian.com/film/article/2024/aug/29/fmovies-shut-down>

4. **Ensure Technical Precision**—Any enforcement action should be narrowly tailored to avoid collateral damage, using methods that do not interfere with core Internet infrastructure.

5. **Collaborate with the Technical Community**—Engage early with Internet infrastructure operators, technical experts, and service providers when designing enforcement policies. Collaboration at this level helps ensure that regulatory goals can be met without introducing unnecessary technical risk, service disruption, or unintended consequences. The technical community can help identify targeted, effective approaches that preserve the integrity of the Internet while supporting legitimate enforcement objectives.

6. **Preserve Resolver Neutrality**—DNS resolver operators should not be compelled to act as national content filters.⁷² Protecting the neutrality of these services is essential to preserving the global interoperability of the Internet.

DNS service providers do not store or curate content and cannot remove infringing material at its source. Blocking at this layer merely disrupts user access—often at the cost of global service stability—while leaving the content intact and pushing users toward insecure circumvention tools.

If content removal is the objective, enforcement efforts should be directed at the entities best positioned to take targeted, proportionate action—such as hosting providers or content platforms.

72

Quad9, “The Public Risk of Governments Controlling DNS Providers,” Quad9 Blog, March 24, 2025.
<https://quad9.net/news/blog/the-public-risk-of-governments-controlling-dns-providers/>



8. CONCLUSION AND A PATH FORWARD

The health and integrity of the global Internet depend on measured, technically sound policy choices. As this report details, blunt interventions frequently fail to achieve their intended goals and often introduce greater harm—economically, socially, and structurally.

Moving forward, we commit to building a living body of evidence. The appendix provides a framework for ongoing case reporting, and we encourage stakeholders to contribute incidents and analysis. With continued collaboration, we can develop effective, focused, transparent, and accountable policies that preserve the Internet as a secure, interoperable, and open system for all.

9. APPENDIX: FRAMEWORK FOR FUTURE REPORTING ON OVERBLOCKING AND FRAGMENTATION

To build on this report and maintain an evolving body of evidence, we invite stakeholders to contribute additional case studies using the template below. Future editions of this report will incorporate new submissions, updates, and data trends. If left unchecked, technical blocking will continue to erode the foundational trust and interoperability that make the Internet possible.

[Country Name]—[Short Title of Incident]

- **Date of Incident:** *(Approximate or ongoing issue?)*
- **Blocking Mechanism Used:** *(DNS, IP, protocol filtering, algorithmic enforcement, etc.)*
- **Intended Target:** *(Copyright infringement, security concerns, political content, etc.)*
- **Collateral Damage:** *(Who else was affected? What services were disrupted?)*
- **Technical Impact:** *(How did it break Internet functionality?)*
- **Sources and Documentation:** *(News articles, technical reports, member testimony, etc.)*
- **Context:** *(Any additional information you can share with us to help us tell the story)*

Send submissions to the Internet Infrastructure Coalition at blockreport@i2coalition.com.