Policy Brief: Perspectives on Internet Content Blocking

September 2025

Executive Summary

Imagine trying to prevent people from entering a building in a city by shutting down an entire street. That street might also be used by hospitals, schools, and homes, so closing it cuts off many essential services for many people, and determined individuals will still find other ways in. This is similar to what happens when governments attempt to block access to specific websites or online content by shutting down parts of the Internet using Domain Name System (DNS) or Internet Protocol (IP) address blocking methods. Although this approach may seem quick and straightforward, it often affects more than intended, disrupting other services and failing to address the core issue.

IP and DNS-based blocking have emerged as the most commonly proposed methods due to their apparent simplicity and ease of deployment1., and governments worldwide are increasingly directing Internet Service Providers (ISPs) and DNS resolvers to block access to Internet content they deem illegal or objectionable, such as unauthorized gambling, child abuse material, copyright infringement, and threats to national security. However, these methods often fail to effectively address the root causes of the targeted issues and can cause significant technical disruptions and societal harm.

While content blocking may seem like a quick fix for preventing access to illegal material, it is often ineffective and frequently causes the blocking of legitimate services, impacting both users and businesses. Further, DNS and IP blocking do not remove the content from the Internet, rendering the material still accessible to determined individuals. Attempts to circumvent blocking may put users' privacy, security, and safety at risk.

The Internet Society provided a technical analysis of the most common blocking methods, highlighting their limitations and potential risks. The analysis shows that both techniques are easily bypassed, imprecise, and prone to causing collateral damage. The Internet Society encourages

[1] i2Coalition. *DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet*, June 3, 2025. Available at: https://i2coalition.com/i2coalition-launches-dns-at-risk-report-and-website-to-spotlight-rising-global-internet-infrastructure-abuse/

policymakers to prioritize solutions that tackle harmful content at its source, rather than relying on blunt technical measures that may create negative externalities to the open and global nature of the Internet.

Key Considerations

DNS and IP blocking, by design, interfere with the basic mechanisms that allow users to find and reach information on the Internet. Implementing DNS and IP-based blocking involves more than just technical execution. These approaches impact how the Internet functions at a foundational level, and their use can lead to significant operational, legal, and societal consequences. This section outlines critical factors that should inform any policy consideration of content blocking.

IP-based blocking denies access to content by preventing the establishment of TCP/IP connections to specific IP addresses, effectively cutting off communication with targeted servers. **DNS-based blocking**, on the other hand, manipulates the Domain Name System by returning false or misleading responses when a user attempts to access a blocked domain, making the content appear unreachable.

Both approaches are typically mandated at the national level and usually implemented within the Internet Service Provider (ISP) network. They are favored in policy circles for their apparent simplicity and scalability. However, these techniques may lack precision and are easily circumvented by users through VPNs (virtual private networks) or changing DNS resolvers, while content providers can just change the infrastructure on which the content is hosted.

What ultimately defines the issue is the gap between the underlying intended policy outcomes and the actual technical effects. These methods do not remove content from the Internet, nor do they address its source. Instead, they impose access barriers that are unreliable and prone to collateral damage. This mismatch between policy goals and technical realities underscores the need for more nuanced, effective, and less disruptive responses.

Challenges

Implementing DNS and IP-based blocking raises a range of complex technical, social, economic, and political challenges. At the technical level, these measures are inherently blunt instruments that struggle to distinguish between illegal and legitimate content when both are hosted behind the same IP address or resolvable on the same domain. As a result, lawful services are often caught in the crossfire, leading to over-blocking and the risk of disrupted access to essential information and platforms.

Imagine a server hosting both a pirate streaming site and a small e-commerce site using the same IP address. An order to block that IP will also block access to the e-commerce site, disrupting legitimate

business operations even though the site had no involvement in piracy[2]. This illustrates how IP-level blocking can trigger broad service disruptions far from the original intent.

In an attempt to regain access, users may turn to tools like VPNs or different DNS resolvers. The danger is that users, in attempting to circumvent content blocking, may inadvertently choose VPN or DNS resolvers that promise access but offer poorer security and privacy protections. As a result, those users' Internet experience may be less safe and secure. Legitimate businesses may be forced to move their services to an unblocked IP address or domain, or a different hosting provider.

Between 2024 and 2025, Italy rolled out its "Piracy Shield" system, an aggressive anti-piracy scheme requiring ISPs, DNS services, and VPN providers to block domains and IPs linked to illegal sports streaming within 30 minutes of rightsholders' requests[3]. However, this policy repeatedly over-blocked legitimate services, including Google domains, Cloudflare-hosted sites, and Google Drive**,** causing widespread disruption for businesses, everyday Internet users, and cloud services[4].

Domain blocking at the level of public DNS resolvers can have unintended consequences that extend beyond content control, directly affecting the online safety of users in countries where these services operate. For example, public recursive resolvers such as Quad9[5] play a critical role in protecting users from malware, phishing, and other cyber threats by filtering harmful domains based on global threat intelligence feeds.

When governments mandate these resolvers to divert technical and operational resources to implement content-specific blocks, it can undermine their core security functions. This not only weakens the protective shield for individuals and businesses but may also reduce a country's overall cyber resilience by removing or impairing a trusted infrastructure layer. The risk is that, in pursuing site-specific enforcement, authorities inadvertently erode a defensive service that benefits millions of users, leaving them more exposed to online fraud, identity theft, and network attacks.

From an economic perspective, DNS and IP blocking measures can impose substantial costs on Internet Service Providers and network operators. These costs include operational expenses for implementing and maintaining blocking systems, revenue losses for online platforms and businesses affected by over-blocking, and broader economic inefficiencies caused by reduced trust and reliability in Internet infrastructure[6].

---

[2] The i2Coalition, *DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet*, May 2025, p. 8, available at: https://i2coalition.com/wp-content/uploads/2025/05/DNS-at-Risk-How-Network-Blocking-and-Fragmentation-Undermine-the-Global-Internet.pdf.

[3] TechRadar, *Italy's Piracy Shield may be breaching EU law…*, July 10, 2025

[4] DediRock, *Report Highlights Risks of Government DNS Blocking*, June 2025

[5] Quad9. *About Quad9*. Available at: https://quad9.net/about

[6] Analysys Mason, *The economic cost of network blocking*, report for Cloudflare, 28 July 2025. Available at: https://www.analysysmason.com/consulting/reports/network-blocking-economic-impact-jul25/

Guiding Principles and Recommendations

The Internet Society believes the most appropriate way to counteract illegal content and activities on the Internet is to address them at their source. Using DNS or IP-address to block access to online content is likely to be ineffective and is prone to causing collateral damage affecting innocent Internet users. For these reasons, and the challenges outlined above, we advise against content blocking. Nonetheless, these techniques are still used. Recognizing this reality, we suggest two main strategies for policymakers concerned about illegal content on the Internet:

- **Address the issue at the source:** The least damaging approach for the Internet is to "attack" illegal content and activities at their origin. Removing illegal content from its source and undertaking enforcement against the source avoids the negative effects of blocking and is more effective at removing illegal content. Cooperation across jurisdictions and stakeholders is a prerequisite for success, as illegal content online extends beyond national borders and national law.
- **Prioritize and use alternative approaches:** For example:
    - Effective cooperation among service providers, law enforcement, and national authorities may provide additional means to help victims of illegal content, and to take enforcement action.
    - Creating an environment of trust where users receive information on what is legal and what is not can improve self-policing. In some cases (e.g. parental control), empowering user to use filters on their own devices, with their consent, can be effective and least damaging to the Internet.

And we offer the following specific guidelines to lessen the negative impact of content blocking:

- **Rule out all non-blocking options:** First, and foremost, exhaust all practical options to have content addressed at the source, or any other alternative means to blocking. Blocking content should not be pursued simply because it is easier. It should be necessary and proportionate.
- **Be transparent:** There should be transparency about the blocking as well as the underlying objective and content blocking policies. Governments should ensure that affected users are able to raise concerns about negative impacts on their rights, interests and opportunities.
- **Empower users**: Users should be able to filter out illegal or unwanted content on their own devices or networks by ensuring access to online safety tools and digital skills training.
- **Limit the scope:** Block content as locally as possible to minimize the global impact.
- **Involve stakeholders:** Policy development and implementation regarding online content should involve a broad set of stakeholders, including technological, economic, consumer rights, and other specialists, to ensure the appropriate steps are taken to minimize negative side-effects of policies to address that content.

- **Follow due legal process:** Any blocking order of unlawful content must be supported by law, independently reviewed, and narrowly targeted to achieve a legitimate aim. The least restrictive means available to deal with illegal activity should be prioritized. Internet Service Providers or other Internet intermediaries should not become de facto law enforcement agents: they should not be required to determine when conduct or content is illegal.
- **Keep it temporary:** Any blocking measures should be temporary. They should be removed as soon as the reason for blocking ceases to exist. It is quite common for illegal content to be moved to evade blocking measures, yet the measures often remain in place long after the content has moved.

The Internet Society's opposition to DNS and IP-based blocking is rooted in how these techniques undermine the Internet's foundational properties, as defined in the Internet Way of Networking (IWN). These blocking methods disrupt the technical architecture that makes the Internet open, globally reachable, and resilient.

The Internet Society has developed a technical description of these foundational principles. We call this The Internet Way of Networking, a framework that describes what makes the Internet unique from other networks. We built the Internet Impact Assessment Toolkit[7] to help our community of technical, policy, and other experts use this framework. It can help identify where policies, business decisions, regulations, or trends may affect the Internet's unique foundation, or the best practices that help it.

[7] Internet Society. *Internet Impact Assessment Toolkit*, 2020. Available at: https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/