

SAC127

DNS Blocking Revisited

Preface

This is a report to the ICANN Board, the ICANN organization staff, the ICANN community, and, more broadly, the Internet community from the ICANN Security and Stability Advisory Committee (SSAC) describes the technical means of DNS blocking and its effects – both intended and unintended – and offers several recommendations on the subject.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), technical administration matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits. SSAC members participate as individuals, not as representatives of their employers or other organizations. SSAC consensus on a document occurs when the listed authors agree on the content and recommendations with no final objections from the remainder of the SSAC, with the exception of any withdrawals included at the end of the document.

Table of Contents

Preface	2
Table of Contents	3
List of Figures	4
Executive Summary	5
1 Introduction	7
2 Examples of DNS Blocking and Motivations	10
2.1 For Security	11
2.2 To Control Access to Content Within an Organization	11
2.3 To Block Access for Legal or Political Reasons	12
3 DNS Blocking: Principles and Assumptions	16
3.1 Blocking Can Be Ineffective or Partially Effective	18
3.2 Over-Blocking and Collateral Damage	18
3.2.1 Case Study: Over-Blocking in Italy's Piracy Shield	21
3.3 Blocking Trains Users to Disable or Ignore Security Controls	22
3.4 Block Evasion Undermines Traffic Visibility and Security Controls	22
3.5 Disclosure and Transparency	23
3.6 Detecting and Measuring DNS Blocking	24
4 Blocking Methods and Implementations	25
4.1 Domain Blocking at a Recursive Resolver	25
4.2 Domain Suspension at Authoritative Nameservers	27
5 Detecting and Circumventing DNS Blocking	29
5.1 Alternative DNS Resolvers	29
5.2 VPNs	29
5.3 Anonymization and Obfuscation Tools	31
5.4 Decentralized Hosting	32
5.5 Use of DNSSEC	32
6 Evolutionary Changes and Trends	33
6.1 Public Resolvers	33
6.2 Government-Sponsored Resolvers	35
6.3 Changes in the DNS Landscape	36
6.4 Blockchain-Based Domains	37
6.5 Encrypted DNS: DoH, DoT, and DoQ (Collectively, DoX)	37
6.6 Extended DNS Error	39
7 Recommendations	40
8 Acknowledgments, Disclosures of Interest, and Withdrawals	40
8.1 Acknowledgments	40
8.2 Disclosures of Interest	42
8.3 Withdrawals	42

List of Figures

Figure 1: The path of a query through a DNS server that has implemented DNS blocking

Figure 2: Screenshot of cracked.io domain seizure

Figure 3: Circumventing DNS blocking by using a VPN, or a public DNS resolver

Figure 4: Measurement of the use of Open Resolvers 2019-2024 (*APNIC Labs*)

Figure 5: Advertisement for Cloudflare's 1.1.1.1 app, which incorporates its public DNS resolver

Figure 6: Image of Apple's iCloud Private Relay

Executive Summary

The Domain Name System (DNS) translates human-readable domain names to Internet Protocol (IP) addresses that are used by computers to communicate with each other on the Internet. DNS blocking is a method for restricting access to information or services on the Internet by interfering with the normal process of responding to DNS queries about domain names or IP addresses. This is done either by denying that a name or address exists or by providing false information about it. Blocking is one of several approaches to restricting or regulating access to Internet information. Often, DNS blocking is employed because it is relatively easy to implement, but it has limitations and potential side effects.

This report focuses on the technical means by which DNS blocking can be accomplished, and the effects—both intended and unintended—of its use in different contexts. The aim of this report is to advise the Internet community, and especially policymakers and government officials, of the implications and consequences of using DNS blocking to control access to resources on the Internet.

DNS blocking can be accomplished by changing the behavior of a DNS server so that it responds in a way that is different from normal, e.g. as was intended by the administrator of the domain name. When an end user wishes to connect to a web site or other service, a recursive resolver translates the domain name of that site or service into an IP address. DNS blocking via recursive resolvers modifies or blocks this translation.

DNS blocking is effective only to the extent that users rely on the DNS infrastructure where the blocking is implemented. Blocking can be bypassed by various methods, such as using an alternative DNS resolver to avoid a resolver where a block has been implemented or using a Virtual Private Network (VPN). The effectiveness of DNS blocking is often a matter of degree.

It is crucial to understand that DNS blocking does not remove or alter the underlying content - it merely attempts to prevent access through the most common and convenient pathway. The content itself typically remains available at the original IP address or through alternative domain names or protocols, meaning that determined users can still reach it using other means.

DNS blocking can have serious side effects. A block may affect users outside the jurisdiction of the party doing the blocking. Users may not know that a block is in place, and can interpret it as a site outage or other error, encouraging potentially insecure behavior to "fix" it. A block may affect domains that provide services for other domains, causing collateral damage beyond the intended scope of the block.

Governments use DNS blocking for complex purposes, and these can be controversial. One motivation is public safety, such as blocking domains that a government decides enable illegal

activities or incite violence. Some governments use DNS blocking as a tool for censorship. The SSAC notes that whether an action constitutes censorship, or the legality of any specific case of DNS blocking, will depend upon local laws (which vary widely across the globe), and can involve personal convictions, about which people may vary in good faith. For these reasons, the SSAC does not make statements in this report about the propriety of specific cases of DNS blocking—such discussions are more suited for political fora. The merits or advisability of governmental or other attempts to control access to resources on the Internet are beyond the scope of this report.

The SSAC makes the following recommendations:

Recommendation 1: SSAC recommends that any entity implementing or mandating DNS blocking understand the implications of the technology.

Recommendation 2: SSAC recommends that DNS blocking implemented by any entity—by a government or any organization that has policy, legal, or operational control over a network or service—follow these guidelines:

- A. The entity should determine whether DNS blocking will fulfill its objectives.**
- B. The entity should have a clear policy about what and how it will block, with well-defined review and decision-making processes that minimize risk.**
- C. The entity should implement the policy using a technique that minimizes overblocking or collateral damage that could affect its users.**
- D. The entity should not affect networks or users outside its administrative control.**

Recommendation 3: SSAC recommends that operators of recursive servers use DNS Extended Error codes (see section [6.6 Extended DNS Error](#)) to indicate to end users and troubleshooters that DNS blocking is taking place.

This report updates SAC050, "DNS Blocking: Benefits vs. Harms,"¹ and SAC056, "SSAC Advisory on Impacts of Content Blocking via the Domain Name System,"² which were published in 2011 and 2012, respectively. Since then, relevant Internet technologies and practices have evolved, and more examples of DNS blocking have been implemented.

¹ ICANN Security and Stability Advisory Committee (SSAC), SAC050: "DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee on Blocking of Top Level Domains at the Domain Name System," June 14, 2011,

<https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-050-en.pdf>.

² ICANN Security and Stability Advisory Committee (SSAC), SAC056: "SSAC Advisory on Impacts of Content Blocking via the Domain Name System," October 9, 2012,

<https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-056-en.pdf>.

1 Introduction

Domain Name System (DNS) blocking is a technique that restricts access to domain names or Internet Protocol (IP) addresses and the content or services associated with them, either by blocking the queries or redirecting them to a different destination.

DNS blocking is a tool—a means that can serve different ends, fueled by different motivations. This tool can be wielded with varying degrees of effectiveness and precision, which can be situational. DNS blocking can have side effects and unintended consequences.

It is important that any entity mandating or implementing DNS blocking understands the implications of the technology. For example, DNS blocking in one jurisdiction can affect the accessibility of content in another jurisdiction. Legal authorities should form technically informed views about DNS blocking, and understand if, or the extent to which, DNS blocking may accomplish their goals and how it may affect parties outside their jurisdictions.

It is important to understand that DNS blocking does not remove the content or service from the Internet. Instead, it prevents a set of users from accessing the content using the domain name. DNS blocking can therefore be a more limited alternative to disabling (suspending) a domain name. Suspending a domain name removes a domain name from the DNS and prevents it from working for anyone, anywhere on the Internet, while blocking might have a much more localized and targeted impact.³

There are various ways in which DNS blocking can be implemented.

A *recursive resolver* receives DNS requests from clients and sends responses. The information contained within these responses is obtained from authoritative DNS name servers. This process is called "resolution."⁴ Many different recursive resolvers exist on the Internet, and each obtains information to be used to satisfy client requests independently.

One of the most common ways to implement DNS blocking is at the recursive resolver (Figure 1). The resolver may be configured to behave in one of several ways. For example, the resolver can be configured to:

- Respond, with an answer that says that the domain does not exist (NXDOMAIN).
- Respond, redirecting the intended traffic from the user to an alternative destination. The user may be informed that the actual destination of interest has been blocked, which informs the user that the actual destination of interest has been blocked.

³ See the "Domain Suspension" section below.

⁴ P. Mockapetris, "RFC 1034: Domain Names – Concepts and Facilities," *ISI* November 1987, Section 2.4.
<https://datatracker.ietf.org/doc/html/rfc1034>

- Redirect the intended traffic from the user to a blackhole destination, which drops all traffic.
- Drop the request.

All of these methods prevent a user from arriving at the Internet destination and/or receiving the content that they requested. The domain name itself continues to function normally for users of other recursive resolvers that do not block the domain.

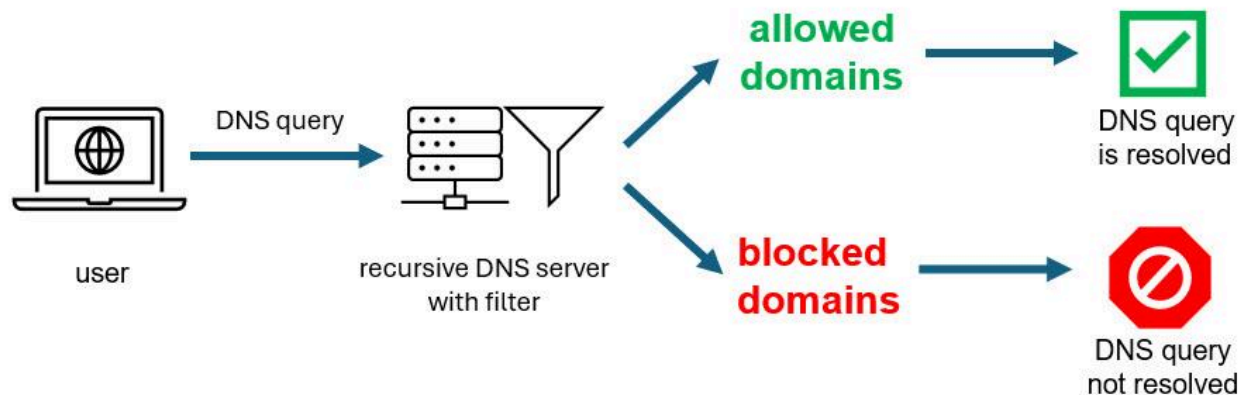


Figure 1: The path of a query through a DNS server that has implemented DNS blocking

Another approach to implement DNS blocking is to use active traffic interception “on the wire,” as opposed to on the recursive resolver. In this method, DNS queries for blocked domain names are intercepted and passed to a DNS filtering process. This filtering process may discard the query, or generate a synthetic DNS response to the query that indicates that the queried name does not exist, or by providing a false IP address, as noted above.

DNS blocking can be applied to domains throughout the DNS namespace. Operators can block entire Top Level Domains (TLDs) (e.g. .tld), and/or second-level domains, (e.g. example.tld), and/or third level domains, (e.g. example.example.tld), and so on. Note that blocking at a specific subdomain level (e.g. example.example.tld) will not affect higher levels (e.g. example.tld or .tld), while blocking at the higher level will typically block anything below that level (e.g. blocking example.tld will block example.example.tld).

Why do parties perform DNS blocking? Generally the goal is to prevent a defined set of users from accessing specific content or a service. The party performing the blocking may not have the desire or authority to prevent a given domain from resolving for everyone on the Internet, and/or the

party performing the blocking may not have the ability to prevent the domain from resolving for everyone on the Internet.

Parties use DNS blocking to serve their needs. For example:

- Corporations and educational institutions restrict access to various types of websites on their devices or networks, because they consider those sites to be distractions or in violation of their acceptable use policies.
- Caregivers may wish to restrict minors within a household from viewing inappropriate content.
- A network operator or a service they use may consider a domain name to be a security threat, and therefore block access to it as a way to protect the service's users.
- DNS blocking is sometimes mandated by government authorities, or it may be required by legal process such as a court order, to block activity that is deemed illegal or harmful.

Network operators and providers of Internet services are usually not obliged to accept all the traffic that is directed toward them, or to allow access to all resources outside their control. Each network operator or service provider has technical control (and usually a legal right) to manage what occurs on its network or service.

A domain name and the content it provides may be legal to serve or to access in one jurisdiction, but not in another. While one jurisdiction may find that it is allowable and desirable to block a domain name, another jurisdiction may consider blocking that domain to be a violation of human or civil rights.

DNS blocking can therefore present controversial situations and unintended consequences, such as when:

- Blocking affects users beyond the jurisdiction of the party doing the blocking.
- A party "over-blocks" a domain—for example by blocking a domain at the second level, when the problematic activity is occurring on the third level—and therefore affects the availability of non-problematic content or service.
- Affected users do not understand that a domain is being blocked, or why. They may interpret the situation as a site outage or other error.
- The blocking is done without users' consent, as opposed to when the blocking is voluntary.

The effectiveness of DNS blocking is often a matter of degree, and some parties who employ DNS blocking may see partial effectiveness as a success.

Governments exercise sovereignty over their territories and the users within them, and may use DNS blocking. A legal jurisdiction is traditionally defined by geography—but the Internet's topography does not align with geography or political borders, and thus, the Internet does not lend itself to precise geographical blocking. In SAC056, SSAC noted that "due to the Internet's architecture, blocking by domain name can be easily bypassed by end users and is thus likely to be largely ineffective in the long term and [is] fraught with unanticipated consequences."⁵ Motivated users can bypass DNS blocking in various ways, such as by using VPNs⁶ or by choosing a different DNS resolver service. Content can be moved to other domains, staying ahead of blocking efforts.

The 2023 open letter "Concerns over DNS Blocking" by Vinton Cerf and other Internet technology and policy experts critiqued draft bills in France, which included a proposal to mandate DNS blocking in certain circumstances.⁷ The signatories highlighted that users can bypass restrictions using alternative DNS resolvers or VPNs, merely redirecting them to potentially less secure systems. The authors also warned that while DNS blocking as a security control to protect users from illegal or malicious websites has "always remained voluntary due to the extraterritorial implications and immense potential for government overreach... the same DNS blocking infrastructure designed to combat online fraud, ransomware, and botnet attacks could just as easily be adapted to suppress internal dissent, censor outside information, and surveil dissidents and journalists."

"DNS blocking" and "DNS filtering" are sometimes used as synonyms. There does not exist a single accepted definition for each that clearly distinguishes them. In this document they are considered synonyms, and everything discussed in this report applies to both equally.

2 Examples of DNS Blocking and Motivations

The intended purposes of or motivations for DNS blocking vary widely, but fundamentally DNS blocking attempts to restrict access to information or a destination on the Internet.

⁵ ICANN Security and Stability Advisory Committee (SSAC), SAC056: "SSAC Advisory on Impacts of Content Blocking via the Domain Name System," October 9, 2012,

<https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-056-en.pdf>.

⁶ A Virtual Private Network (VPN) establishes a digital connection between a user's computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts personal data, masks the user's IP address, and lets the users bypass website blocks and firewalls on the Internet. For more about them, see the "VPN" section below. For an expanded description of a VPN, see Paul Ferguson and Geoff Huston, "What is a VPN?" April 1998, <https://www.potaroo.net/papers/1998-3-vpn/vpn.pdf>.

⁷ Vinton Cerf, Stephen D. Crocker, et al: "Concerns Over DNS Blocking" *Medium* June 24, 2023. <https://medium.com/@vgcerf/concerns-over-dns-blocking-988ef546a100>.

2.1 For Security

The use of DNS blocking for security and anti-abuse purposes is pervasive, and most Internet users and organizations are protected via DNS blocking. This DNS blocking is an important and proven tool for protecting users and helping keep the Internet and specific services safer in the face of cybercrime, fraud, and other detrimental activities.

A DNS blocklist is a list of domain names that the user of the list will not process further, or will process in a certain way.^{8,9} A common use is to block access to or traffic from domains controlled by malicious actors, such as malware and phishing sites.

All major email providers use domain name blocklists to filter out phishing, malware, spam, and scam emails.¹⁰ Some public DNS resolvers use blocklists to protect their users from Internet threats.¹¹ The major web browsers use blocklists to warn users of malicious sites, including Google Chrome, Microsoft Edge, Mozilla's Firefox, DuckDuckGo, and Apple's Safari. Google states that billions of devices are protected via its Google Safe Browsing technology, which is a blocklist of domain names and URLs.¹² Companies build blocklist-powered protective systems into apps and social media offerings. Companies such as Cisco, NordLayer, Zvelo, and Cloudflare offer services that allow customers to use DNS blocklists to filter network traffic and block connections to malicious domain names, and such solutions (provided as services) are widely used by companies, Internet Service Providers (ISPs), governments, universities, and other organizations.

2.2 To Control Access to Content Within an Organization

It is common for organizations to use DNS blocking to shield their users on their networks from content and services determined by the organization to be inappropriate.

Educational institutions such as schools and libraries employ DNS blocking to limit access to content deemed inappropriate or harmful, such as those related to gambling, pornography, or

⁸ For descriptions of blocklists and how they work, see: Greg Aaron and Dave Piscitello, "Reputation Block Lists: Protecting Users Everywhere," <https://www.icann.org/en/blogs/details/reputation-block-lists-protecting-users-everywhere-1-11-2017-en>, Siôn Lloyd, ICANN Office of the Chief Technology Officer, "RBL Evaluation Methodology," <https://www.icann.org/en/system/files/files/octo-037-04dec23-en.pdf>, and Matt Stith, "DNS Blocklist Basics," November 11, 2020, <https://www.spamhaus.org/resource-hub/email-security/dns-blocklist-basics/>.

⁹ These are sometimes called "Reputation Blocklists" or "RBLs."

¹⁰ Including Gmail, Yahoo!, Microsoft, GMX, Zoho, Twilio's Sendgrid, and MailChimp. Spamhaus claims that its blocklists protect 4.5 billion mailboxes. See: https://content.spamhaus.org/spamhaus_brand_guide.pdf.

¹¹ For example, Quad9 describes its service thusly: "When your computer performs any Internet transaction that uses the DNS (and most transactions do), Quad9 blocks lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets, and it can improve performance in addition to guaranteeing privacy." <https://quad9.net/>.

¹² "Google Safe Browsing: Transparency Report." <https://transparencyreport.google.com/safe-browsing/overview?hl=en>.

violence.¹³ Schools may restrict access to game sites and social media platforms in the hope that students' time is spent productively and in line with educational goals.

Similarly, companies may use DNS blocking to restrict access to content and services by employees, enforcing these rules throughout the company infrastructure. Some employers restrict access to social media and dating sites, gambling sites, pornography, and other "not suitable for work" content and services in an attempt to maintain workplace productivity, reduce potential legal liabilities, and foster a professional workplace environment.¹⁴

Some households also use parental control and child-protection solutions, which can be installed on devices or on the household's local network.

Government offices and other organizations sometimes restrict employees from accessing content and services to mitigate the accidental or purposeful dissemination of sensitive information.

2.3 To Block Access for Legal or Political Reasons

Governments use DNS blocking for complex and sometimes far-reaching purposes. One motivation is public safety, such as blocking domains that the government finds are used to promote illegal activities, incite violence, or spread misinformation. Some governments use DNS blocking as a tool for censorship, limiting access to information that it deems subversive, politically destabilizing, or challenging to the status quo.

Whatever the case, the controversial content may be hosted outside the jurisdiction that finds the content problematic. A government may have no legal or practical way to prevent the material from being made available on the Internet—for example by having the content removed at the hosting provider, or by suspending the domain and making it stop resolving. That government may therefore shift to preventing access to the material from within the jurisdiction, and DNS blocking can provide a means to accomplish that goal.

In recent years there have been new examples of government-mandated DNS blocking, and DNS blocking has been the subject of continuing legislation and litigation. These illustrate legal and political motivations for DNS blocking, and how jurisdictions exercise their sovereignty over the Internet and the users within their jurisdictions. Below are a few notable examples.

¹³ For example, see the U.S. "Children's Internet Protection Act (CIPA)," *FCC* updated July 5, 2024, [https://www.fcc.gov/consumers/guides/childrens-internet-protection-act#:~:text=Children%27s%20Internet%20Protection%20Act%20\(CIPA\)%20%7C%20Federal%20Communications%20Commission](https://www.fcc.gov/consumers/guides/childrens-internet-protection-act#:~:text=Children%27s%20Internet%20Protection%20Act%20(CIPA)%20%7C%20Federal%20Communications%20Commission).

¹⁴ For example, "No Fun While Browsing at Work. What Content do Employers Block the Most?," *NordLayer* March 20, 2024, <https://nordlayer.com/blog/what-content-employers-restrict-to-employees/>. See also, "Telus Cuts Subscriber Access to Pro-Union Website," *CBC*, July 24, 2005. <https://www.cbc.ca/news/canada/telus-cuts-subscriber-access-to-pro-union-website-1.531166>.

One of the best-known and most impactful examples of government-mandated blocking is the "Golden Shield Project," also referred to as the "Great Firewall of China." This is the system used by the People's Republic of China to restrict access to Internet content and Internet destinations by all users located within mainland China. First implemented in 1998, this system utilizes various means to filter and block content according to government guidelines, at scale. The system is used to block entire domains and services, including those of prominent sites such as Google.com, Wikipedia, Facebook, X (formerly Twitter), and Dropbox. China blocks content at the infrastructure level, where incoming content is filtered (at the IP packet level) by government authorities at the points where traffic traverses the national border. The system also manipulates content by scanning for certain keywords and phrases;¹⁵ blocks by IP ranges; and employs DNS redirection, injecting forged DNS replies.^{16,17}

In June 2022, Switzerland's Federal Supreme Court gave its approval to a DNS blocking strategy introduced by Switzerland's Intercantonal Lottery and Betting Commission in 2019, and rejected claims that the blocking is unconstitutional. The blocking was designed to block access within Switzerland to three Malta-based online gambling sites that were illegal to use within Switzerland under Switzerland's Gambling Act 2018. The court found the DNS blocking to be proportionate in restricting the access of individuals in Switzerland to online gaming offerings that are not authorised in Switzerland. The court found the system to wield a sufficiently preventive effect on Swiss nationals who attempt to access unlicensed operators, and that it is more effective than alternatives.¹⁸

In September 2024, Brazil's Supreme Court upheld a judicial order banning access in Brazil to social media platform X, because X was not complying with Brazilian law.¹⁹ The order required Brazil's telecommunication agency, ISPs, and mobile providers to block access, and imposed fines

¹⁵ For example see: "When is the Internet Not the Internet?," *Internet Society* December 1, 2023, <https://www.internetsociety.org/resources/internet-fragmentation/the-chinese-firewall/>; "Great Firewall Report," <https://gfw.report/>; and Melissa Brachfeld, "MC2 Researchers Circumvent China's Latest Form of Internet Censorship," December 8, 2023, <https://cyber.umd.edu/news/story/mc2-researchers-circumvent-chinas-quos-latest-form-of-internet-censorship>.

¹⁶ Anonymous, "Towards a Comprehensive Picture of the Great Firewall's DNS Censorship," *Usenix*, <https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf>

¹⁷ Philipp Winter and Stefan Lindskog, "How the Great Firewall of China is Blocking Tor," *Usenix*, <https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf>

¹⁸ Richard Mulligan, "Swiss Supreme Court rejects complaint against DNS blocking system." *iGB*, June 28, 2022, <https://igamingbusiness.com/legal-compliance/legal/swiss-supreme-court-rejects-complaint-against-dns-blocking-system/>. See also Fabienne Bretscher and Sandra Marmy, "Switzerland: Swiss Federal Supreme Court approves blocking against foreign providers of online gambling," *Baker McKenzie*, August 10, 2022, https://insightplus.bakermckenzie.com/bm/consumer-goods-retail_1/switzerland-swiss-federal-supreme-court-approve-s-blocking-against-foreign-providers-of-online-gambling

¹⁹ João da Silva and Vanessa Buschschlüter, "Top Brazil court upholds ban of Musk's X," *BBC*, September 2, 2024, <https://www.bbc.com/news/articles/crkmp53l6jo>

for users who accessed X using VPNs. Implementation varied among providers; some reportedly blocked the X.com domain.²⁰

In 2022, in judgments related to three linked lawsuits, a U.S. federal court ordered all Internet service providers in the United States to block the domains of three pirate streaming services.²¹ The lawsuits were filed by Israeli TV and movie producers and providers against Doe defendants who were "re-broadcasting and streaming Plaintiffs' original content, broadcasting channels and TV services which are only authorized for broadcasting and/or viewing in the territory of the State of Israel and under a license." The court found the blocking proper because the content was not authorized for streaming within the United States. The court found the blocking necessary because the defendants used domain names in various TLDs and at various registrars and could switch domains, and because "Defendants have gone to great lengths to conceal themselves and their ill-gotten proceeds from Plaintiffs' and this Court's detection, including by using multiple false identities and addresses associated with their operations and purposely deceptive contact information for the infringing Website." The court's order required U.S. ISPs to block access to the websites "by any technological means available on the ISPs' systems. The domain addresses and any Newly Detected Websites shall be channeled in such a way that users will be unable to connect and/or use the Website, and will be diverted by the ISPs' DNS servers to a landing page operated and controlled by Plaintiffs (the "Landing Page")."²² Here the DNS blocking would hamper access to the content within the United States, but would not block access to the content in other countries. The court's solution did not seek to suspend the domain names themselves, leaving them resolvable outside the United States.

In Venezuela, the government intensified digital censorship ahead of 2024's elections,²³ employing DNS and Hypertext Transfer Protocol Secure (HTTPS) blocking to suppress websites. Some users responded by relying on VPNs or alternative DNS resolvers.

Recent intellectual property lawsuits have led to court decisions involving public resolvers. (For more about these, see the "Public Resolvers" section below.) These resolvers are used by people in

²⁰ Lily Hay Newman, "Why It's So Hard to Fully Block X in Brazil," *Wired*, September 5, 2024, <https://www.wired.com/story/brazil-x-ban-isp-blocking/>.

²¹ John Brodtkin, "Every ISP in the US Must Block These 3 Pirate Streaming Services," *Ars Technica*, May 3, 2022, <https://arstechnica.com/tech-policy/2022/05/judge-rules-every-isp-in-us-must-block-pirate-sites-run-by-mysterious-defendants/>.

²² Default Judgment and Permanent Injunction Order, Case 21 Civ. 11024, United States District Court, Southern District of New York, April 22, 2022. <https://storage.courtlistener.com/recap/gov.uscourts.nysd.572373/gov.uscourts.nysd.572373.49.0.pdf>

²³ Robbie Mitchell, "Internet Censorship Verging on Service Blocking Ahead of Venezuela Elections," *Internet Society Pulse*, July 26, 2024, <https://pulse.internetsociety.org/blog/internet-censorship-verging-on-service-blocking-ahead-of-venezuela-elections>, and Freedom House "Freedom on the Net" report, June 1, 2023 to May 31, 2024, <https://freedomhouse.org/country/venezuela/freedom-net/2024>.

multiple countries, so this DNS blocking would affect the users of these resolvers in many jurisdictions, and would not affect users of other DNS resolvers. Three examples are:

- **Cloudflare Public Resolver (1.1.1.1):** In an Italian case at the Court of Milan in November 2022, three music torrent sites under an in-country blocking order were found to be accessible through Cloudflare's public DNS resolver (1.1.1.1), and the court ordered Cloudflare to also block access to these sites.²⁴ Cloudflare appealed the decision, stating that blocking at the public resolver would lead to over-broad blocking outside the jurisdiction of the order. The appeal was dismissed and the original blocking order remained in place.
- **Cloudflare Public Resolver (1.1.1.1):** In November 2024, the Higher Regional Court of Cologne in Germany, in *Universal v. Cloudflare*, rejected a request, based on allegations of online copyright infringement, to require Cloudflare's public DNS resolver to block a music piracy website's domain. This was an opposite result from the Italian case above. However, the court affirmed the lower court judgment requiring Cloudflare to block access to the domain at issue through its CDN and pass-through security service.
- **Quad9 Public Resolver (9.9.9.9):** Quad9 was served with a demand in December 2023 from Italy, to block music piracy sites that were accessible via its public resolver.²⁵ Quad9 appealed this decision, but in the meantime blocked access to those sites while the appeal process was ongoing. Quad9 noted: "We have complied with the request, and these names are now blocked on Quad9 systems. Since the courts have provided again no guidance on how we determine if a request is made by someone under Italian jurisdiction, we have applied this block globally."

A research team composed of academic and commercial members measured how ISPs in different EU countries attempted to enforce political sanctions through DNS blocking. The research found a wide variation in the effectiveness of the blocking and coverage, both internationally and within individual member states. The researchers concluded that "the inconsistent implementation of the sanctions can at least in part be attributed to the high-level description of the sanctions and the lack of recommendations for technical implementation."²⁶

²⁴ Ernesto Van der Sar, "Court Upholds Piracy Blocking Order Against Cloudflare's 1.1.1.1 DNS Resolver," *TorrentFreak*, November 9, 2022, <https://torrentfreak.com/court-upholds-piracy-blocking-order-against-cloudflares-1-1-1-1-dns-resolver-221109/>.

²⁵ "Italian Blocking Demands: Following a Bad Example," *Quad 9*, December 6, 2023, <https://quad9.net/news/blog/italian-blocking-demands-following-a-bad-example>

²⁶ John Kristoff, Moritz Müller, et al: "Internet Sanctions on Russian Media: Actions and Effects." 2024. <https://dataplane.org/jtk/publications/kmfrko-foci-24.pdf>

3 DNS Blocking: Principles and Assumptions

DNS blocking has limits and potential consequences. Entities who may implement DNS blocking should consider their goals and whether blocking will satisfactorily meet those goals, and should weigh those goals against potential side-effects.

There are several advantages to DNS blocking. It is relatively simple to implement and can be broadly effective across large networks, in large part because it covers all devices connected to a network without needing to install software on each device. Since DNS queries are one of the first steps in accessing any content or service, blocking can prevent the access early, saving bandwidth and processing time.

However, there are also practical limitations to DNS blocking. There are several effective methods that users can employ to bypass or circumvent it, each with its own strengths depending on the user's technical proficiency and needs:

- A user can configure the use of a different DNS service, such as a public DNS resolver, that does not impose the same restrictions.
- Users can bypass some methods of DNS blocking by protecting their DNS traffic through various forms of encryption or obfuscation.
- Users can use Virtual Private Networks (VPNs) to encrypt all Internet traffic and effectively routing all traffic, including DNS traffic, around the DNS blocking.

DNS blocking may predominantly affect users who are less technically savvy and are not aware of these methods.

DNS blocking is only effective if the user relies on the DNS infrastructure of the entity implementing the block. For more, see "Circumvention Methods and Tools" below.

The providers of the content and services being blocked can also take steps to ensure availability in spite of the blocking. For example, a provider can move the content to a different, unblocked domain name. For more, see "Decentralized Hosting" below.

DNS blocking may motivate content or service providers to work around these blocks; DNS blocking may be only partially or temporarily effective, and "success" is a matter of degree.

DNS blocking can result in overblocking, where the blocking extends to content, services, or users it was not meant to (or should not) affect. Blocking can be an unnecessary or disproportionate means to achieve the purported aim, if the blocking is not sufficiently targeted, and can infringe

upon the access and rights of users who are not under the jurisdiction that ordered the blocking.^{27,28} For more, see the "Over-Blocking" section below.

All technical approaches to DNS blocking, and attempts to circumvent the blocking, can have some impact on users and applications. At worst, they may have an effect on the security or stability of an important service. Regardless of the mechanism used, SSAC suggests that entities that order or implement blocking should apply the following principles. Here an "entity" can be a government, a company, or other type of organization that has policy, legal, or operational control over a network or service:

1. The entity determines whether the blocking policy will fulfill its objectives.
2. The entity implements the policy using a technique that minimizes overblocking or collateral damage that could affect its users.
3. The entity makes a concerted effort to not affect networks or users outside its administrative control.

When these principles are not applied, DNS blocking can negatively affect parties not under the administrative control of the entity, and those parties may not have a recourse.

SAC050 suggested that the first principle of practicing medicine – *primum non nocere* ("first, do no harm") – should also apply to Internet technology and practices.²⁹ In the case of DNS blocking, "doing no harm" means creating no circumstances where Internet users or content outside of the entity's administrative control are adversely affected by the entity's policy or implementation. The SSAC suggests approaches that produce the fewest unintended consequences and the least harm outside the blocked domain.

If some content or service is deemed to be unacceptable, then the most effective response may be to take it down at its source—such as at the hosting provider. However, this option assumes that the source of the problematic content can be controlled, directly or indirectly, by the same public authority that has deemed the content or service to be unacceptable.

²⁷ For example see: Anonymous, "The Collateral Damage of Internet Censorship by DNS Injection," *Computer Communication Review* Vol 42 No 3 (2012): 21-27 <https://dl.acm.org/doi/pdf/10.1145/2317307.2317311>.

²⁸ One expression of principles regarding the right to freedom of expression on the Internet, and the effect of DNS blocking on it, is: Frank La Rue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 16 May 2011, A.HRC.17.27., https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

²⁹ ICANN Security and Stability Advisory Committee (SSAC), SAC050: "DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee on Blocking of Top Level Domains at the Domain Name System," June 14, 2011, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-050-en.pdf>, pp. 4-5.

3.1 Blocking Can Be Ineffective or Partially Effective

As noted above, there are tools to circumvent DNS blocking. Even non-technical users can easily use VPNs, encrypted DNS, and public resolvers. In addition, these circumvention activities are by their nature difficult to track, and so authorities may assume that their blocking is effective when it is not.

The result is that some number of users will be able to get around the blocking, and blocking may never be 100% effective. Government authorities who require blocking should understand that the effectiveness of blocking will be a matter of degree, and should not expect that ISPs and network operators will be able to use DNS blocking to completely prevent access to a given piece of content, domain, or service.

For example, when Brazil's Supreme Court ordered that X.com be blocked in Brazil in 2024, the blocking took effect over time, and may not have been complete. Brazil has about 20,000 ISPs, and only a few of them have infrastructure nation-wide. While the main Internet providers implemented the block quickly, some observers' telemetry indicated there was a long tail of local and regional ISPs where X.com remained available for several days. ISPs also used varying techniques to implement the ban.³⁰ Brazilians' use of VPNs to access X became an issue during the ban.³¹

3.2 Over-Blocking and Collateral Damage

Parties may make errors in the list of domains (or IP addresses, or URLs) they block. This may affect unrelated parties, or may adversely affect the blocker's own users. The SSAC does not take a view on what exact management process is best – it will vary depending on the organization and its goals – but SSAC does recommend that the authority have clear guidelines about what and how it will block, and well-defined review and decision-making processes that minimize risk.

In any filtering regime, whether in the DNS or elsewhere, it is important to avoid errors when generating a list of domains for blocking. The core list for types of domains that should be blocked is called the “ground truth” list. This list is made and maintained based on the specific industry and use case. Error is defined against that list, and erroneous entries on a blocklist are known as false positives. False positives can impose costs on the party performing the blocking, and on users affected by the blocking. The risks associated with false positives can grow as the number of affected users increases.³²

³⁰ Lily Hay Newman, "Why It's So Hard to Fully Block X in Brazil," *Wired*, September 5, 2024, <https://www.wired.com/story/brazil-x-ban-isp-blocking/>.

³¹ Reuters, "Fact Check: Brazilians Can Be Fined for Using VPNs to Access X," September 6, 2024, <https://www.reuters.com/fact-check/brazilians-can-be-fined-using-vpn-access-x-2024-09-06/>.

³² Siôn Lloyd, ICANN Office of the Chief Technology Officer, "RBL Evaluation Methodology," <https://www.icann.org/en/system/files/files/octo-037-04dec23-en.pdf>

Precision in the selection process is important. For example, if a party believes that problematic content is located on the second-level domain name *example.TLD*:

- If the party blocks *.TLD*, it will block all domains in the TLD, which may include many more services and content than intended.
- If the party blocks *example.TLD*, it blocks everything at and beneath that domain. If *example.TLD* or *third-level.example.TLD* provides service to other domains, those domains may also be affected.
- The blocking will affect all services that use DNS lookups, including Web, email, network management, and file transfers that use the blocked domain.³³

A well-known example of such over-blocking is the Mooo.com case. The second-level domain Mooo.com was used to provide about 84,000 third-level domains (*example.mooo.com*), on which thousands of users hosted content of many different kinds. A small number of those third-level domains hosted child abuse and counterfeit goods content. In an attempt to block access to the illegal material, a government agency received permission to seize the second-level domain Mooo.com and redirect it to a warning page. This disrupted all of the subdomains, making all content unavailable and adversely affecting Mooo.com's innocent site users, until the mistake was reversed.^{34,35}

A typographical error during data entry can both fail to block the intended domain name and accidentally block an unrelated domain. Internationalized domain names (IDNs) can pose special hazards since two different IDNs can appear to be identical to a user but will always be distinct in the DNS (and in nycode).

Blocking can also be performed heuristically, such as with a machine learning classifier. The classifier might use characteristics of a DNS query such as the source IP address, whether the domain has ever been seen before or blocklisted, website content, or other pre-collected information. This essentially creates a blocklist "on the fly." With such methods, it can be difficult to predict whether a blocked name actually has malicious content, or merely exhibits statistical similarity to a previously blocked name.. Such systems may require significant reliability testing

³³ See: Rogue, "#OrangeIsTheNewBlacklist: In France Google and Wikipedia Briefly Censored for 'Apologia of Terrorism,'" *Medium*, October 18, 2016, <https://medium.com/@maliciarogue/in-france-google-and-wikipedia-briefly-censored-for-apologia-of-terrorism-60a3f16fb9a7>; Suresh Ramasubramanian, "Microsoft's Takedown of 3322.org-A Gigantic Self Goal?," *CircleID*, September 17, 2012, https://circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/; and Mike Masnick, "ICE Finally Admits it Totally Screwed Up; Next Time, Perhaps It'll Try Due Process," *Techdirt*, February 21, 2011, <https://www.techdirt.com/2011/02/21/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process/>.

³⁴ David Piscitello, "The Value of Assessing Collateral Damage Before Requesting a Domain Seizure," ICANN org, January 24, 2013, <https://www.icann.org/en/system/files/files/seizure-collateral-assess-24jan13-en.pdf>.

³⁵ Ernesto Van dewar Sar, "U.S. Government Shuts Down 84,000 Websites, 'By Mistake,'" *Torrentfreak*, February 16, 2011, <https://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/>.

before deployment in a production environment. It may be challenging to define and maintain an acceptable false-positive rate, and false-positives may need to be examined manually in order to train the system.

Blocking domains that provide DNS name services for other domains can be particularly impactful. If applied to a major authoritative DNS infrastructure domain, considerable parts of the Internet can become unresolvable to the blocked users.

We note that some providers have blocked entire TLDs on their services or networks. Some do this because they feel that abuse in the TLD has become pervasive, and they find it easier (or less risky) to simply block the entire TLD.^{36,37,38,39} Other providers assign risk scores to certain TLDs, which can make it more likely that second-level domains in the TLDs will be blocked on the service. Once the reputation of a TLD or a second-level domain has been harmed, it can be difficult to repair the damage. TLD operators should be aware of factors that can affect abuse levels and therefore the reputation of a TLD, such as pricing, registrant verification and validation,

³⁶ .XXX was originally proposed as a TLD that could be blocked entirely by those wishing to prevent access to pornographic materials. See "Universities block triple-X domain names," *ABC News*, December 12, 2011, <https://abcnews.go.com/Technology/universities-block-triple-domain-names/story?id=15136644>.

In its rationale for approving the .XXX TLD, the ICANN Board stated: "The issue of governments (or any other entity) blocking or filtering access to a specific TLD is not unique to the issue of the .XXX sTLD. Such blocking and filtering exists today. While we agree that blocking of TLDs is generally undesirable, if some blocking of the .XXX sTLD does occur there's no evidence the result will be different from the blocking that already occurs." See ICANN Board's "18 March 2011 Rationale for Approving Registry Agreement with ICM's for .XXX sTLD," <https://www.icann.org/en/system/files/bm/draft-icm-rationale-18mar11-en.pdf>.

The blocking of the .XXX TLD was built into filtering software and browser extensions. See "Technical Specifications," *Metacert Protocol*, https://metacertprotocol.com/assets/metacert_technical_paper.pdf

³⁷ Anti-spam systems have long offered their users the ability to filter out entire TLDs. For example, this can be accomplished via SpamAssassin rules, and Microsoft Exchange settings.

³⁸ A number of companies offer their customers the ability to block entire TLDs in their networks, including BlueCat, SafeDNS, and Palo Alto Networks, which offers its External Dynamic List feature so that "Palo Alto Networks customers have the opportunity to block individual TLDs entirely when they deem them inappropriate."

See: "Which top-level domains to block and how to do it right," *BlueCat*, 3 April 2024, <https://bluecatnetworks.com/blog/which-top-level-domains-to-block-and-how-to-do-it-right/>; Val Redman, "Top-level Domains Blocking Guide," *SafeDNS*, February 2, 2020, <https://blog.safedns.com/top-level-domains-blocking-guide/>; Janos Szurdi, "A Peek into Top-Level Domains and Cybercrime," *Unit 42*, November 11, 2021, <https://unit42.paloaltonetworks.com/top-level-domains-cybercrime/>.

³⁹ Governments sometimes block TLDs on their networks, to protect government workers. For example, the U.S. government's Cybersecurity & Infrastructure Security Agency (CISA) recommended that non-federal organizations use protective Domain Name System (pDNS) resolvers or similar mechanisms to "block rarely used top-level domains (TLDs) with suspicious characteristics" to prevent phishing.

See "Capacity Enhancement Guide: Counter-Phishing Recommendations For Non-Federal Organizations," *CISA*, January 12, 2021, https://www.cisa.gov/sites/default/files/2023-09/CISA_CEG_Counter-Phishing_Guidance_for_Non_Federal_Orgs%20Aug-23%20Revision.pdf.

abuse prevention and mitigation, and registrar relations and distribution management.^{40,41,42,43} As SSAC noted in SAC115, "Abuse at scale is a pervasive problem that erodes trust in the overall ecosystem," and "The primary point of responsibility for the management (including abuse management) of a TLD lies with the registry operator."⁴⁴

3.2.1 Case Study: Over-Blocking in Italy's Piracy Shield

Italy instituted its Piracy Shield program, in which the country's telecom regulator, AGCOM, has the right to designate certain domains and IP addresses as piracy sites. All in-country Internet providers and VPN services are required to block access to those sites in automated fashion, via IP blocking and/or DNS poisoning. On October 19, 2024, AGCOM and Piracy Shield listed the domain name *drive.usercontent.google.com*, a subdomain for the CDN of Google's Milan node, and a critical domain that supports the functioning of Google Drive. As a result, this prevented users in Italy from being able to download files stored on Google Drive for several hours, until the mistake was withdrawn. YouTube also used the CDN, so the accessibility of YouTube across Italy was also affected. While Piracy Shield operates an allow list, apparently important subdomains of major providers were not on it, according to investigation by Wired Italy.⁴⁵

This was a case of erroneous blocking. The subdomain did not exclusively host illegal content and was a component of a widely used commercial service.

The Italian law also had some commercial consequences. One VPN provider, Aircom, decided to withdraw offering its service in Italy, claiming that the Piracy Shield program was "too burdensome for AirVPN, both economically and technically."⁴⁶

⁴⁰ For analysis of factors that affect abuse levels in TLDs, see: Maciej Korczyński, Maarten Wullink, Samaneh Tajalizadehkhoob, Giovane C.M. Moura, Cristian Hesselman, "Statistical Analysis of DNS Abuse in gTLDs Final Report," August 9, 2017. <https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf>.

⁴¹ For analysis of factors that affect abuse levels in TLDs, see: "Cybercrime Supply Chain 2024: Measurements and Assessments of Cyber Attack Resources and Where Criminals Acquire Them," *Interisle Consulting Group*, November 18, 2024, <https://static1.squarespace.com/static/63dbf2b9075aa2535887e365/t/67448fb0ca887f100bc60f4e/1732546482023/CybercrimeSupplyChain2024.pdf>.

⁴² Ram Mohan, "Which Domains Stand the Strongest Against Phishing Attacks?" *CircleID*, December 8, 2014, <https://circleid.com/posts/8604/10424/>.

⁴³ Regarding gTLD security and anti-abuse services as a tool for reputation and "enhancing trust and protecting" a national internet community, see: ".au Completes Historic Transition to Afilias," *PR Newswire*, June 30, 2018, <https://www.prnewswire.com/news-releases/au-completes-historic-transition-to-afilias-300675091.html>.

⁴⁴ SAC115: "SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS," 19 March 2021, pages 18 and 21, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf>

⁴⁵ Raffaele Angius and Luca Zorloni, "Stavolta Piracy Shield l'ha fatta grossa e ha bloccato Google Drive" ("This time Piracy Shield has gone too far and blocked Google Drive"), *Wired.it*, October 19, 2024, <https://www.wired.it/article/piracy-shield-blocco-google-drive-download/>.

⁴⁶ "Termination of Service in Italy," *Air VPN*, February 5, 2024, <https://airvpn.org/forums/topic/57256-termination-of-service-in-italy/>.

3.3 Blocking Trains Users to Disable or Ignore Security Controls

DNS blocking through redirection will usually result in Transport Layer Security (TLS) errors for websites, which may trigger warnings and interstitial pages in browsers. The only way for users to proceed will be for them to click "Ignore," which trains users to ignore name mismatch certificate errors.

3.4 Block Evasion Undermines Traffic Visibility and Security Controls

DNS data gives Internet Service Providers (ISPs) an important and accurate picture of both traffic patterns and security threats on their networks. This information can allow an ISP to identify increases and shifts in traffic, which can inform business decisions. Even more importantly, monitoring DNS data supports network security, often enabling ISPs to diagnose denial-of-service attacks and identify infected hosts, compromised domains, and vulnerable users/customers.

When users turn to alternative DNS servers, some network operators, ISPs, and enterprises may experience decreased ability to manage security threats and manage certain network operations. For example, if a user accesses the third party recursive resolver via an encrypted connection using DNS over HTTPS (DoH) or DNS over TLS (DoT) and is infected with malware, the user's ISP may not be able to detect that and notify the infected user, since DNS telemetry is being diverted away from the ISP.⁴⁷ Furthermore, the set of Internet configuration attributes that need to be evaluated when a customer calls an operator help desk for support will be more extensive, and will increase both cost and debugging complexity.

Government-mandated domain blocking can encourage end users to take steps to ensure their DNS traffic is routed through nameservers outside the country. This "off shore" routing of domain name queries can transfer DNS observability and control to other countries, frustrating anti-cybercrime activities within the country implementing the blocking. In addition to the additional latency that may be incurred, this external routing of DNS traffic can also have an impact on Internet performance within the blocking nation, since many Content Delivery Networks (CDNs) make decisions regarding what information to return on DNS queries based on the source IP address of the resolver making the query. The use of non-local servers can result in unexpected traffic traversing international links.

When users employ circumvention techniques, parties lose some ability to gain evidence and intelligence information from network and Internet service operators. For example, ISPs and the U.S. Federal Bureau of Investigation relied on DNS telemetry about infected machines during Operation Ghost Click, a significant action that shut down servers that propagated the

⁴⁷ "Call for Comments – Development of a Network-level Blocking Framework to Limit Botnet Traffic and Strengthen Canadians' Online Safety," Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), March 15, 2021, p. 9, https://www.m3aawg.org/sites/default/files/m3aawg-response-to-crtc_march_15_2021.pdf.

DNSChanger malware.⁴⁸ Modern circumvention techniques can reduce the amount of such telemetry, making it harder to identify infected machines and impairing remediation efforts.

3.5 Disclosure and Transparency

Disclosure that DNS blocking is taking place – and transparency as to which domain names are being blocked – can be desirable and appropriate in some cases. In practice, however, DNS blocking policies and actions are often not disclosed to affected parties, including to end users. This can make it difficult for end-users to understand when they are being blocked, or why.

Absent some level of transparency, DNS blocking can be difficult to recognize for what it is. It can be misdiagnosed as a hosting outage, a misconfiguration, or a malicious attack. End users, network administrators, service providers, and other parties may spend time attempting to find the root cause of the problem, and may make mistaken attempts to mitigate the problem.

Entities such as public resolvers may state whether they perform DNS blocking. However, it may be impractical for such parties to reveal the exact lists of domains that they block, for reasons including:

- Revealing what domains they are blocking places them at a defensive disadvantage. Operators often do not want to reveal their operational practices to aggressors such as cybercriminals.
- Lists of blocked domains tend to change rapidly, and can be large (such as with reputation block lists).
- Some reputation blocklists are provided under a legal license, and thus cannot be published publicly in their entirety.

Some legal authorities that order or perform blocking intentionally do not offer transparency about what domains are being blocked, or why, while others publish lists.^{49,50}

Some commercial DNS blocklists are transparent about whether any given domain is on their lists, and have transparent procedures for requesting the removal of domains from their lists. This

⁴⁸ Elgan, Mike, "How the DNSChanger Shutdown Changed Cybersecurity." SecurityIntelligence, 14 November 2022. <https://securityintelligence.com/articles/how-dnschanger-shutdown-changed-cybersecurity/>

⁴⁹ The Federal Service for Supervision of Communications, Information Technology and Mass Media (*Roskomnadzor*) is the Russian federal executive agency responsible for monitoring, controlling, and censoring Russian mass media. Roskomnadzor maintains an official mandatory list of blocked domains (and URLs and IP addresses). <https://eais.rkn.gov.ru/en/>

⁵⁰ France's LOPPSI 2 law requires that French Internet service providers block access to an address if authorities consider that this is required to prevent the distribution of pornographic images of minors. The Ministry of Interior notifies ISPs which sites to block. The list from the Ministry of Interior remains confidential, because the authorities do not want to publicly advertise the locations of this kind of site. [https://www.loc.gov/item/global-legal-monitor/2011-03-22/france-new-law-on-internal-security-loppsi-2/#:~:text=The%20Law%20criminalizes%20online%20identity,2.\)](https://www.loc.gov/item/global-legal-monitor/2011-03-22/france-new-law-on-internal-security-loppsi-2/#:~:text=The%20Law%20criminalizes%20online%20identity,2.))

provides confidence for customers, and can help domain owners correct problems on their services.⁵¹

Extended DNS Error Codes have been increasingly used to indicate blocking. SSAC suggests that operators of recursive servers use DNS Extended Error codes (see section [6.6 Extended DNS Error](#)) to indicate to end users and troubleshooters that DNS blocking is taking place.

3.6 Detecting and Measuring DNS Blocking

Measurement efforts have tended to focus on DNS blocking used to implement censorship. Research has documented the challenges of measuring this phenomenon.⁵² This DNS blocking is measured through network monitoring and probes. These can determine whether a domain is being blocked for users who are in different geographical locations and are using different service providers.

One of the largest repositories of data about DNS blocking is held by the Open Observatory of Network Interference (OONI).⁵³ OONI was launched in 2012 as a free software project under The Tor Project, aiming to study global Internet censorship. In 2017, OONI launched OONI Probe, a mobile app that runs a series of network measurements. These measurements detect blocked domains, websites, and applications. Overall, the publicly available OONI Explorer database holds the results of more than two billion network measurements collected from 27,000 distinct networks in 242 countries and territories.⁵⁴ In September 2024, the OONI Probe project performed almost 57 million measurements collected across 2,964 networks in 176 countries.⁵⁵ OONI uses various test methodologies to determine where and how blocking takes place. For example, OONI finds DNS blocking by determining whether DNS responses (such as the IP addresses mapped from host names) performed both over a control server and over the network of the user do not match.⁵⁶

The GFWatch is a large-scale, longitudinal measurement platform that has been continuously monitoring DNS filtering by China since March 2020.⁵⁷ It is capable of testing hundreds of

⁵¹ SURBL and Spamhaus are examples. For more, see Lloyd, "RBL Evaluation Methodology."

⁵² Paul Pearce, et al. "Global measurement of DNS manipulation," (2017) In Proceedings of the 26th USENIX Conference on Security Symposium (SEC'17). *USENIX Association*, USA, 307–323.
https://faculty.cc.gatech.edu/~pearce/papers/dns_usenix_2017.pdf

⁵³ See "Global Community Measuring Internet Censorship Around the World," *Open Observatory of Network Interference (OONI)*, <https://ooni.org/>.

⁵⁴ Maria Xynou, "Russia blocked OONI Explorer, a large open dataset on Internet Censorship," *OONI*, September 25, 2024, <https://ooni.org/post/2024-russia-blocked-ooni-explorer/>.

⁵⁵ See: "Explorer," *Open Observatory of Network Interference (OONI)*, <https://explorer.ooni.org/>.

⁵⁶ See: "Web Connectivity," *Open Observatory of Network Interference (OONI)*, <https://ooni.org/nettest/web-connectivity/>.

⁵⁷ Nguyen Phong Hoang, "GF Watch: A Longitudinal Measurement Platform Built to Monitor China's DNS Censorship at Scale," *Citizenlab*, November 4, 2021, <https://citizenlab.ca/2021/11/gfwatch-a-longitudinal-measurement-platform-built-to-monitor-chinas-dns-censorship-at-scale/>.

millions of domains daily. The project is an academic collaboration between researchers from Stony Brook University, University of Massachusetts - Amherst, University of California - Berkeley, and the Citizen Lab at the University of Toronto. The project lists domains it finds to be blocked.^{58,59}

4 Blocking Methods and Implementations

One of the fundamental elements of the Internet's architecture is the "end-to-end" principle, which minimizes the need for intelligence in the core (middle) of the network but embraces intelligence at the edge (on individual hosts). This architecture has enabled a tremendous range and depth of innovation. Content blocking via the DNS has been implemented sometimes in the Internet "core" and sometimes at the "edge." Connections inside or between operators are "core" connections between an access provider and its traffic sources and traffic sinks are at the "edge." Applications and clients exist toward the edge. An example of edge-based blocking is blocklists in web browsers.

As a result of this architecture, efforts to block traffic at any point in a network other than at the edge can be circumvented, for example by the use of a VPN. Even in cases where complete administrative and operational control over Internet access networks is possible (such as within an ISP or at some Internet exchange points),⁶⁰ end users have still been able to access prohibited content. Motivated users can bypass DNS blocking by changing their DNS provider to one that is not performing DNS blocking, or by using a VPN to use a different DNS service.⁶¹

Various methods of blocking DNS have been proposed or implemented. Some methods pose greater technical concerns than others. A non-exhaustive examination follows.

4.1 Domain Blocking at a Recursive Resolver

Recursive resolvers are a common place to implement DNS blocking, and there are a number of tools (both commercial and open source) that allow resolver operators to easily implement

⁵⁸ See: "Censored Domains," *GFWatch*, https://gfwatch.org/censored_domains.

⁵⁹ For additional background, see: Fenglu Zhang, et al., "Investigating Deployment Issues of DNS Root Server Instances From a China-Wide View," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 6, pp. 5275-5292, Nov.-Dec. 2024, <https://ieeexplore.ieee.org/document/10460172>.

Simone Basso, "Measuring DoT/DoH Blocking Using OONI Probe: a Preliminary Study," *NDSS Symposium*, (2021) <https://censorbib.nymity.ch/pdf/Basso2021a.pdf>.

"DNS Blocking Effectiveness: Recent Independent Tests," *Quad9* May 31, 2020, <https://www.quad9.net/news/blog/dns-blocking-effectiveness-recent-independent-tests/#>.

"Malicious Site Filters on DNS in 2020," *Skadligkod* May 3, 2020, <https://www.skadligkod.se/general-security/phishing/malicious-site-filters-on-dns-in-2020/>.

⁶⁰ See: "Internet Exchange Point," *Wikipedia*, last edited January 15, 2025, https://en.wikipedia.org/wiki/Internet_exchange_point.

⁶¹ Vinton G. Cerf, Stephen D. Crocker, et al., "Concerns over DNS Blocking," *Medium*, June 24, 2023, <https://medium.com/@vgcerf/concerns-over-dns-blocking-988ef546a100>.

blocking. Recursive resolvers, typically operated by the end user's ISP, fetch DNS data from authoritative servers (such as a TLD server) upon request from end users. When an end user wishes to connect to a web site or other service, the recursive resolver serving that end user translates the domain name of that site or service into IP addresses. DNS blocking via recursive resolvers aims to filter, edit, or block this translation. It can be easily bypassed, if the end user configures their system to simply use another recursive resolver.

Blocking at a recursive resolver can be done in a number of ways:

1. **Via Redirection:** In this form of recursive resolver blocking, the response from the authoritative server is modified to substitute values specified by the DNS blocking policy. For example, instead of returning the IP address of the offending web server, the recursive resolver returns an IP address of a remediation server that displays a message indicating the site is being blocked. A DNS injection system forges DNS responses to DNS queries for domain names that are being blocked.
2. **Via a Query Response that Does Not Give An Actual Resolution:** As with redirection, this form of blocking modifies the response from the authoritative server. However instead of returning the IP address of another server (or any other information about the domain name), the response is modified to indicate the requested domain name does not exist ("NXDOMAIN" response, the most common form of this mechanism), or that it is not resolvable for other reasons (responses such as "REFUSED", "SERVFAIL", "NOTIMPL", "FORMERR").
3. **Via Query Non-Response:** Finally, the recursive resolver could be configured to ignore queries for a requested domain. As with REFUSED and other error response codes, the lack of a response might under certain circumstances render the resolver unusable from the perspective of the querier.

Another way to implement DNS blocking is to use active traffic interception “on the wire,” as opposed to at a recursive resolver. In this method, DNS queries for blocked domain names are intercepted by a third-party (“Man In The Middle”) and passed to a DNS filtering process. This filtering process may discard the query, or generate a synthetic (substitute) DNS response to the query that indicates that the queried name does not exist, or provide a false IP address, as noted above.

When blocking a Domain Name System Security Extensions (DNSSEC)-secured domain by substituting the response, the lack of a valid signature allows for detection of the fabricated nature of the response, if the client performs DNSSEC validation itself (which is rare). This observation is independent of where exactly the response is substituted.

4.2 Domain Suspension at Authoritative Nameservers

Operators of authoritative servers can remove a domain name from the zone file, thereby preventing it from resolving. This is often referred to as domain "suspension," especially when talking about second-level or third-level domains that a party has registered at a domain registrar. This phenomenon is *not* DNS blocking. We mention it here because domain suspension is a way to prevent access to a domain (and the content on it), and can serve some of the same goals as DNS blocking.

While DNS blocking leaves the domain in the DNS zone and prevents or redirects resolution for a subset of users, domain suspension prevents a domain name from resolving at all. This affects all users of the domain, and affects all services that operate on the domain. Suspension is therefore a more impactful act than blocking the domain in the DNS.

Domain suspension is a common occurrence. Thousands of malicious second-level domains are suspended every day to address abusive activities such as phishing, malware, and scams.⁶² These suspensions take domains out of the control of the malefactors, and prevent the domains from adversely affecting any users. ICANN's contracts require that registrars and registry operators take action when presented with verifiable cases of DNS abuse, and depending on the circumstances the most appropriate action may be to suspend a domain name.^{63,64} Registrars also suspend significant numbers of domains for non-payment, and when registrants do not confirm their contact data as required.

Technically, suspension is accomplished by removing a domain name from the DNS parent zone from which the domain is delegated (in which it is registered). For domains held in a TLD registry, suspension can be accomplished by the TLD's registry operator, or by the domain's sponsoring registrar. When using the EPP protocol, this involves the registry placing the domain on ServerHold status, or the registrar placing it on ClientHold status. A domain can also be suspended if the registry operator or the registrar removes (dissociates) the nameservers associated with the domain. Once a domain is removed from the zone file via one of these methods, it may take

⁶² For more about the problem of malicious domain registrations, see: Nosyk, Korczyński, et al: "INFERMAL: Inferential Analysis of Maliciously Registered Domains." *ICANN org*, November 8, 2024, <https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf>; For an example of the scale of domain suspensions, see: Transcript of "ICANN78 AGM – GNSO RrSG Membership" held on Tuesday, October, 24, 2023:

https://static.sched.com/hosted_files/icann78/95/TRANSC_I78HAM_Tue24Oct2023_GNSO%20RrSG%20Memship%20%283%20of%203%29-en.pdf?_gl=1*1x9iffh*_gcl_au*OTQ1MjAzNjEwLjE3MzYxMTgyMzU.*FPAU*OTQ1MjAzNjEwLjE3MzYxMTgyMzU, especially pp. 25-26.

⁶³ "Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement," *ICANN org*, February 5 2024.

<https://www.icann.org/resources/pages/advisory-compliance-dns-abuse-obligations-raa-ra-2024-02-05-en>

⁶⁴ ICANN Security and Stability Advisory Committee (SSAC), "SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS," March 19, 2021.

<https://www.icann.org/en/system/files/files/sac-115-en.pdf>

minutes to days for the domain to become unresolvable globally, as the domain expires from DNS caches around the world.

A registrar or registry operator can also effectively "seize" or repossess a domain and change the nameservers associated to the domain, pointing it to different content. Here the domain continues to resolve, but the domain is no longer under the control of its previous registrant. This solution is sometimes employed when domain names are seized by law enforcement via a court order, so that the domain can resolve to an explanatory web page operated by the legal authority. Here the repointing happens for all visitors to the domain—unlike with DNS blocking, which could redirect the domain for only a subset of users.



Figure 2: Screenshot of cracked.io domain seizure.

The cracked.io web site was a cybercrime forum that trafficked in stolen passwords and malware. The domain was seized by the U.S. Federal Bureau of Investigation (FBI) on January 29, 2025 per a court order. Before seizure, the domain was on nameservers cartman.ns.cloudflare.com and treasure.ns.cloudflare.com. At the court's direction, the registry operator changed the nameservers to ns1.fbi.seized.gov and ns2.fbi.seized.gov, pointing the domain to the above notification page.

The colloquial term "domain takedown" can refer to a suspension, or to a legal seizure, or to a redirection order.

When a DNSSEC-secured domain is seized, unless DNSSEC is removed or replaced, the lack of a valid signature allows for detection of the fabricated nature of the response. This observation may not be relevant since the response is intended to be informative and not a substitute for the actual service.

5 Detecting and Circumventing DNS Blocking

There are several methods that users can employ to identify or bypass DNS blocking, each with its own strengths and weaknesses depending on the users' technical proficiency and needs.

5.1 Alternative DNS Resolvers

One of the simplest circumvention methods is to change the DNS settings on a device so that it uses an alternative resolver (or "DNS server") that does not enforce the same blocking restrictions. A "public resolver" or "open resolver" is a DNS resolver that accepts and processes queries from any (or nearly any) client.⁶⁵ Examples include Google Public DNS (8.8.8.8), Cloudflare's public resolver (1.1.1.1), and CIRA's Canadian Shield.⁶⁶ Using a public or alternative resolver is easy to implement and is within the capabilities of all but the most non-technical users, and video tutorials exist that walk users through these processes.

However, this is effective only if access to the alternative DNS resolver itself is not blocked, restricted, or manipulated by the ISP or network administrator on the network path. This is where DNS encryption technologies, such as DNS over HTTPS (DoH) and DNS over TLS (DoT) can be used to bypass on-path interception and manipulation of the DNS. For more, see the "Encrypted DNS" section below.

5.2 VPNs

VPNs have emerged as a popular tool for users who seek greater online freedom and security, as well as for circumventing geographic content restrictions, and for circumventing government-mandated blocking. The increasing demand for VPNs has led to a surge in their availability and adoption by the Internet-using public.

A VPN establishes a connection between a user's computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts personal data, masks the user's IP address, and lets the users bypass website blocks and firewalls on the Internet.⁶⁷

⁶⁵ The term "public resolver" refers to open resolvers that are meant to be open—as compared to open resolvers that are open because they are misconfigured, and should be or were intended to be closed.

⁶⁶ "Free Public DNS for Canadians," CIRA, <https://www.cira.ca/en/canadian-shield/>.

⁶⁷ For an expanded description of a VPN, see Paul Ferguson and Geoff Huston, "What *is* a VPN?" April 1998, <https://www.potaroo.net/papers/1998-3-vpn/vpn.pdf>.

VPNs work by creating an encrypted connection between the user's device and a VPN server, which acts as a proxy between the user and servers on the Internet. This allows users to access the Internet while keeping their private data (such as IP address and therefore location) hidden from the Internet sites that the user visits.

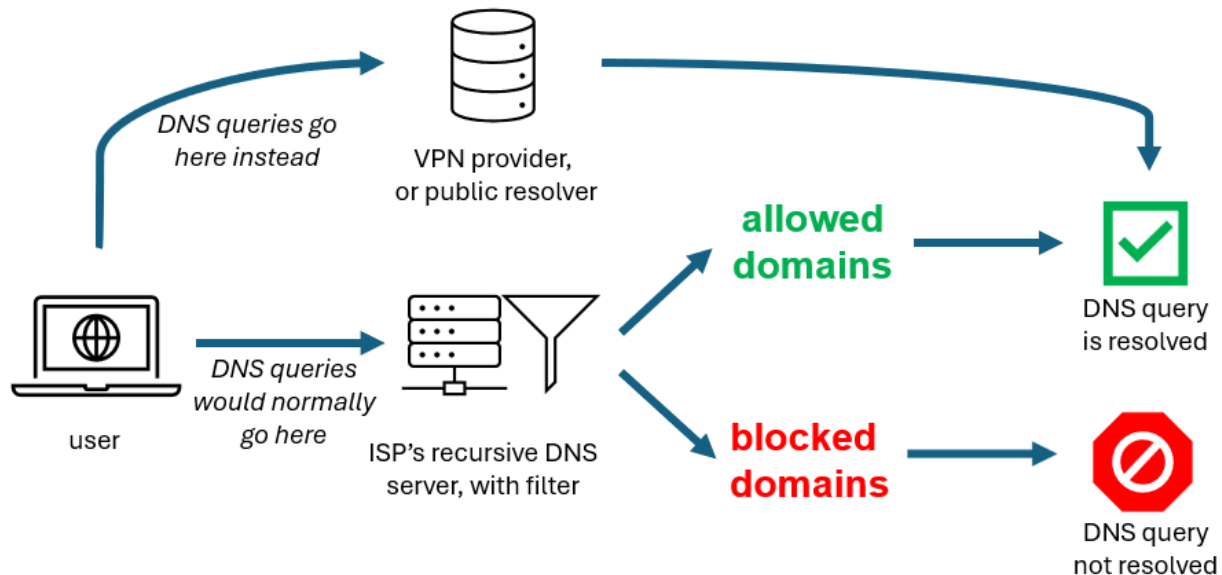


Figure 3: Circumventing DNS blocking by using a VPN, or a public DNS resolver

VPNs offer several key benefits to users:

1. **Bypassing Geo-Restrictions:** One of the primary attractions of VPNs is their ability to mask a user's true location. For example, by connecting to a VPN server in a different country, a user can access content that may be restricted or unavailable in their region. This is appealing to those who wish to view streaming services or websites that are limited to access from specific geographic areas.
2. **Evading Censorship:** By encrypting Internet traffic and routing it through servers in other countries, VPNs allow users to bypass government-imposed restrictions and access information freely.
3. **Enhanced Privacy, and Anonymization:** VPNs encrypt all Internet traffic passing through their servers, making it difficult for third parties, such as ISPs or malicious actors on the path being bypassed, to monitor or intercept user activity. This added layer of privacy is valued by individuals who are concerned about their online data being collected

The technical considerations related to the operation of an IP-based VPN are described in: "RFC 2764: A Framework for IP Based Virtual Private Networks," *Internet Engineering Task Force (IETF)*, February 2000, <https://www.rfc-editor.org/rfc/rfc2764>.

and used without their consent. On the other hand, VPNs are also used by criminals to hide their IP addresses and evade detection.

4. **Secure DNS Resolution:** Many VPN services offer their own DNS resolvers, which further enhances user privacy and security. By handling DNS requests within the encrypted VPN tunnel, VPNs prevent external entities from tracking or manipulating DNS queries. VPNs can also mitigate DDoS attacks and bandwidth throttling.

VPN usage is significant in some regions. In the United States, polls indicate that 46% of respondents use VPNs,⁶⁸ with a comparable percentage in Canada.⁶⁹ The major VPN providers operate thousands of servers each located in multiple countries, and use millions of IPv4 addresses, including some in residential ranges.⁷⁰

The use of VPNs to evade censorship has become a widespread practice, raising concerns among governments and content providers who seek to enforce restrictions and control access to information. This has led to an ongoing cat-and-mouse game between VPN providers and those who seek to block or restrict their use. Blocking VPNs is possible because most VPN protocols have distinct characteristics, such as specific traffic signatures and behaviors, and commercial services maintain lists of VPN IP addresses that subscribers can block. In response, VPN providers have introduced protocols designed to avoid advanced network filtering. Based on web tunnel technology, these make VPN traffic appear indistinguishable from regular web traffic and attempt to blend in with ordinary Internet activity, making it more difficult for network filters to identify.⁷¹

5.3 Anonymization and Obfuscation Tools

The Onion Router (Tor) network offers another powerful tool, particularly for those concerned about privacy, anonymity, and bypassing DNS blocking. Tor anonymizes and encrypts Internet traffic by routing it through multiple nodes around the world, making it difficult for DNS blocks or any other form of surveillance to be effective. Unlike traditional VPNs, which typically route traffic through a single server, Tor's multi-layered approach significantly enhances anonymity and circumventing blocking, as each node in the Tor network only knows the previous and next hop, but not the entire route. This ensures that DNS requests within the Tor network do not go through the user's local DNS servers, effectively bypassing any local DNS blocking measures. However, while Tor is highly effective for privacy and DNS blocking circumvention, it can be slower than regular Internet connections due to its multi-hop architecture, and it may also be blocked by some

⁶⁸ Brett Cruz, "2024 VPN Trends, Statistics, and Consumer Opinions," *Security.org*, September 26, 2024 <https://www.security.org/resources/vpn-consumer-report-annual/#:~:text=Today%2C%2046%20percent%20of%20people,of%20respondents%20just%20last%20year>.

⁶⁹ Aurelija Einorytė, "NordVPN Survey Reveals: Users Still Trust Free VPNs," February 23, 2024, <https://nordvpn.com/blog/nordvpn-usage-survey/>.

⁷⁰ "Tsvetomir Koychev, "The Best VPN Service of 2025," *Techopedia*, December 13 2024, <https://www.techopedia.com/vpn/best-vpn>.

⁷¹ These include NordNet's NordWhisper protocol (<https://nordvpn.com/blog/nordwhisper-protocol/>) and Proton VPN's Stealth protocol (<https://protonvpn.com/blog/stealth-vpn-protocol>)

networks. (The more a Tor exit node is used, and the more it supports suspicious activity, the greater the likelihood that it may be blocked by network operators.) In an attempt to limit online anonymity and circumvention, some governments have blocked access to Tor. In response, the Tor Project designed pluggable transports and an ever-evolving tool suite to disguise Tor traffic and the points of entrance into the Tor network. One example is Tor Snowflake, a pluggable transport that proxies traffic through temporary proxies using Web Real-Time Communication (WebRTC), a peer-to-peer protocol.⁷²

Another circumvention tool is the open-source tool Psiphon.⁷³ It uses a combination of secure communication and obfuscation technologies, such as a VPN, Secure Shell (SSH), and a Web proxy, and a centrally managed and geographically diverse network of thousands of proxy servers, using a performance-oriented routing architecture.

5.4 Decentralized Hosting

Providers of content and services can take steps to ensure availability in spite of DNS blocking. An example of a relevant technology is the InterPlanetary File System (IPFS), a protocol and decentralized data storage and delivery network based on peer-to-peer (P2P) networking.⁷⁴ Instead of having a central server that holds and distributes a website or data file, IPFS is a decentralized system of user-operators who hold copies of data. Any user in the network can serve a file by its content address, and other peers in the network can find and request that content from any node that has it.

IPFS has been used to host websites and content that are resistant to blocking and takedown, such as when Turkey ordered the blocking of Wikipedia in 2017.⁷⁵ IPFS is also used by criminals, to make phishing sites more resistant to takedown.⁷⁶

5.5 Use of DNSSEC

DNSSEC is a set of enhancements to the DNS that provides the receiver of a response to a query a means to detect “spoofing,” including data origin authentication (“did this DNS response really come from the *example.com* zone?”) and data integrity checking (“did a man-in-the-middle

⁷² For more information, see: “Snowflake,” *TOR Project*, <https://snowflake.torproject.org/> and “TOR Snowflake,” *OOONI*, <https://ooni.org/nettest/tor-snowflake/>.

⁷³ For example, see: “Psiphon” www.psiphon.ca.

⁷⁴ For descriptions of IPFS, see: “What is IPFS?” *IPFS*, <https://docs.ipfs.tech/concepts/what-is-ipfs/>.

⁷⁵ Brady Dale, “Turkey Can’t Block This Copy of Wikipedia,” *Observer*, May 10, 2017, <https://web.archive.org/web/20171018092720/http://observer.com/2017/05/turkey-wikipedia-ipfs/>.

⁷⁶ Interisle Consulting Group (Greg Aaron, Lyman Chapin, David Piscitello, Karen Rose, and Colin Strutt), “Phishing Landscape 2024,” July 23, 2024, pp. 19-20. <https://static1.squarespace.com/static/63dbf2b9075aa2535887e365/t/66cde404c8345e766972319c/1724769286084/PhishingLandscape2024.pdf>.

attacker modify the data in this response after it was signed?”). When DNSSEC is applied to a domain, such validation protects clients from being misled by spoofed responses.

If a client performs the DNSSEC validation itself, it will detect that a domain is being spoofed or that no response is available (depending on the configuration and specific failure that occurs).⁷⁷ If multiple resolvers are configured on the client, each one will be tried in turn, until an unmodified response is obtained or the available options are exhausted, effectively blocking the requested resource. In that case, a technically capable user might pursue another path to obtain the blocked response, such as configuring their client to use an additional resolver not subject to blocking.

In practice, most clients depend on a separate recursive resolver to perform DNSSEC validation. In those configurations, clients trust their resolver to provide accurate responses. When the resolver itself performs the blocking, it can claim that the queried domain did not use DNSSEC, or that the response actually did validate when it did not. In this situation, clients are bereft of any means to detect the trust violation.

6 Evolutionary Changes and Trends

In recent years there have been a variety of technical, social, and political developments relevant to DNS blocking.

6.1 Public Resolvers

The landscape of DNS resolution has undergone a remarkable transformation in recent years, characterized by a significant rise in the popularity and utilization of public DNS resolvers. These resolvers, offered by various providers, have garnered widespread adoption due to their ability to deliver fast, reliable, and accurate DNS responses. Users are aware of the benefits of public DNS resolvers and have been reconfiguring their systems to leverage these services. This shift has been fueled by a growing understanding of the potential privacy and performance advantages that public resolvers offer over default DNS configurations, and in response to cases of state censorship and the abuse of DNS services offered by ISPs.

Measurements by APNIC Labs have shown that about 21% of Internet users appeared to be using public resolvers as of December 2024:

⁷⁷ This is assuming that the parent of the blocked domain is DNSSEC signed, which is true for all gTLDs and the overwhelming number of ccTLDs.

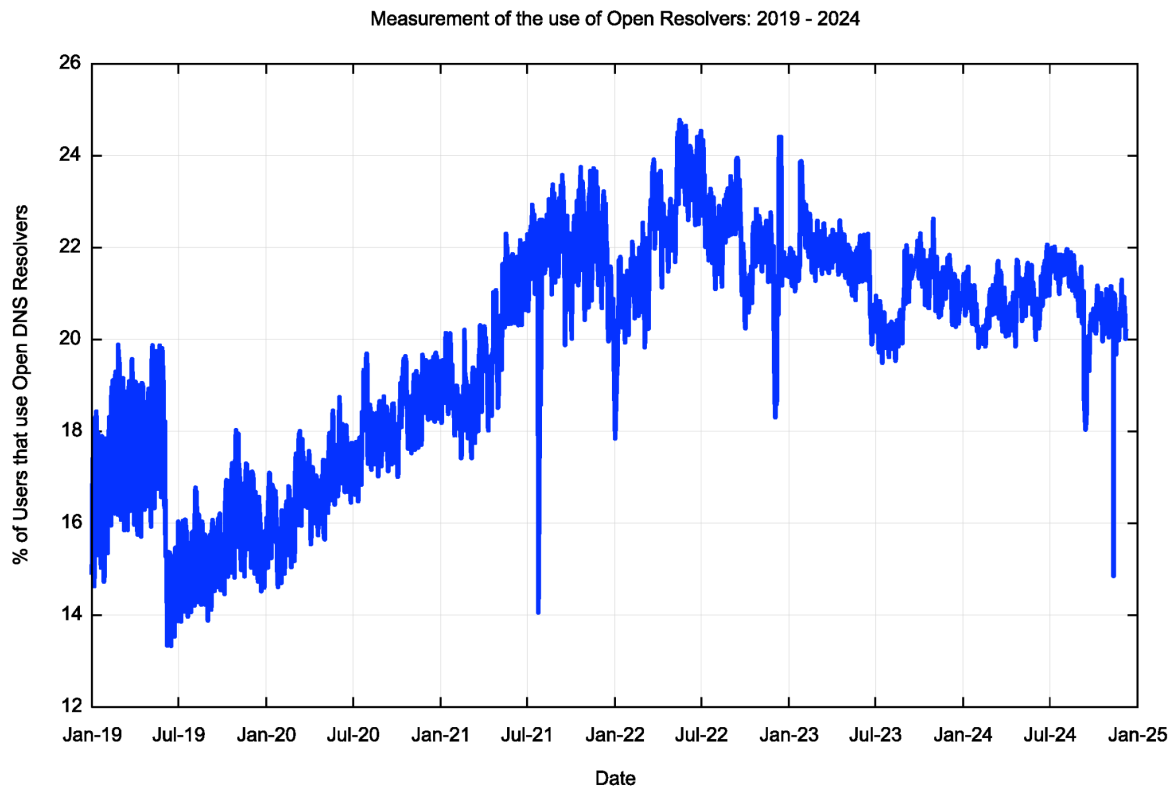


Figure 4: Measurement of the use of Public Resolvers, 2019-2024 (*APNIC Labs*)⁷⁸

Several factors have contributed to the increased accessibility and user-friendliness of public DNS resolvers. Notably, services like Cloudflare's 1.1.1.1 have simplified the configuration process, making it easier for users to switch to their resolvers.

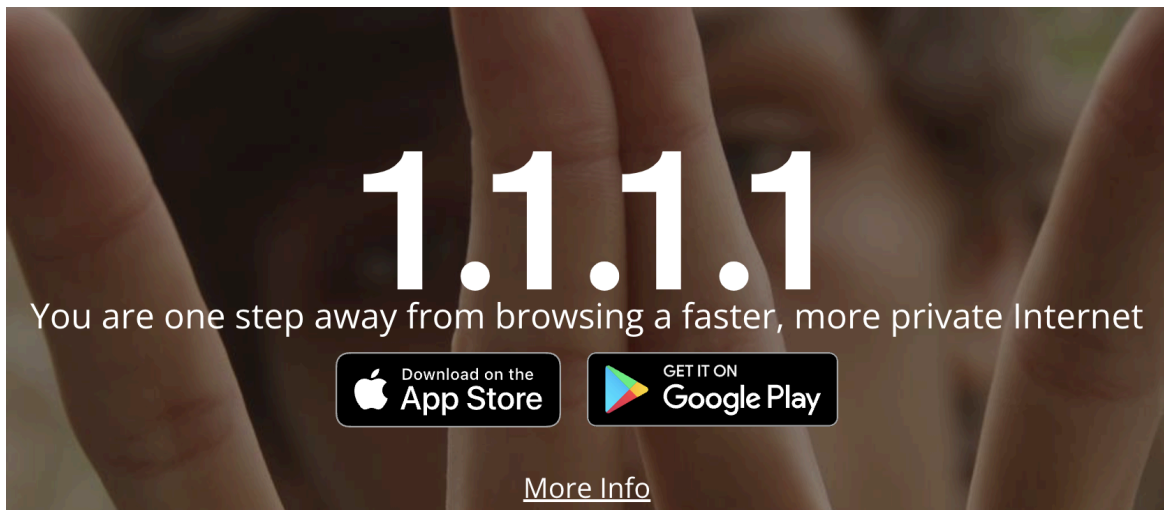


Figure 5: Advertisement for Cloudflare's 1.1.1.1 app, which incorporates its public DNS resolver

⁷⁸ Image courtesy of *APNIC Labs*, <https://labs.apnic.net/measurements/>.

Additionally, Apple has integrated its Private Relay feature⁷⁹ directly into Apple devices, further driving the adoption of alternative DNS resolution options.

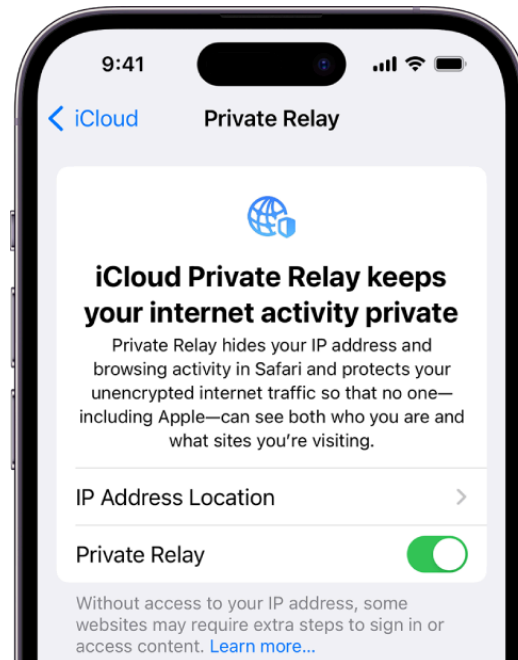


Figure 6: Image of Apple's iCloud Private Relay

A trend towards utilizing multiple public resolvers gathered momentum over the period 2018 - 2022. Users apparently recognized the advantages of redundancy and load balancing by configuring their systems to use several resolvers in a failover mode. This approach enhanced reliability by ensuring that DNS queries were answered even if one resolver experienced issues.

6.2 Government-Sponsored Resolvers

A trend is that governments are funding DNS resolvers, designed to protect users from harm. Examples include:

- **DNS4EU:** This initiative, funded by the European Commission, "aims to offer an alternative to the public DNS resolvers currently dominating the market,"⁸⁰ based on a recommendation in the NIS2 directive.⁸¹ The main goals are to increase protection against cybersecurity threats, and provide "a privacy-compliant, and resilient DNS service to strengthen digital sovereignty and security for EU citizens, governments, and critical infrastructure."⁸² It will offer several options for different users: a free and voluntary-use

⁷⁹ "About iCloud Private Relay," *Apple* August 31, 2023, <https://support.apple.com/en-us/102602>.

⁸⁰ "About the Project," *DNS4EU*, <https://www.joindns4.eu/about>.

⁸¹ "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), *EUR-Lex*, Item 100, <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>.

⁸² "Join the European Safe Digital Space," *DNS4EU*, <https://www.joindns4.eu/>.

DNS resolver for the public, a version for telcos (to "process the complete DNS traffic on those resolvers" for their users' traffic), and a version for government users.

- **Protective Domain Names Service (PDNS):** a project overseen by the U.K.'s National Cyber Security Centre (NCSC), launched in 2017.⁸³ It is designed to protect against malware, phishing, and other cybersecurity threats by preventing access to domains known to be malicious, by simply not resolving them. It has been mandated for use by central government departments, and is available to local governments, schools, and emergency services, but not to the private sector. Approximately 7.2 million individual users used the system in 2023.⁸⁴ In 2022, PDNS handled 810 billion DNS queries, and blocked 11 billion DNS queries related to 420,000 domains, or about 2% of all queries made.⁸⁵
- **Cybersecurity & Infrastructure Security Agency (CISA):** In the U.S., CISA's Protective DNS Resolver Service is a "device-centric service that secures and blocks government web traffic from reaching malicious destinations, and alerts security organizations within agencies when incidents occur."⁸⁶

6.3 Changes in the DNS Landscape

The ICANN Name Collision Analysis Project Study 2 Report (NCAP 2) enumerated multiple changes in the DNS landscape, as a way to understand where and how name collisions occur.⁸⁷ These DNS evolutionary changes also have relevance in DNS blocking.

The primary evolutionary changes include: the use of new DNS transports (such as DNS-over-TLS, DNS-over-HTTPS, and DNS-over-QUIC), additional DNS privacy extensions (such as QNAME minimization and Oblivious DNS), and features that address both privacy and query volume, such as aggressive Next Secure Record (NSEC) and local root instances. These changes may result in non-symmetric system usage and also hide the information necessary to determine which domain is being queried.

⁸³ Sean O'Rourke, "NCSC announces new partnership for PDNS delivery," *4th Platform*, April 19, 2024, <https://4thplatform.co.uk/2024/04/19/ncsc-announces-new-partnership-for-pdns-delivery-2-2/>.

⁸⁴ "UK Protective DNS (PDNS)," *Nominet*, <https://nominetcyber.com/delivering-uk-pdns/>.

⁸⁵ "Active Cyber Defence: The Sixth Year," *National Cyber Security Centre (UK)*, <https://www.ncsc.gov.uk/files/ACD6-full-report.pdf>.

⁸⁶ "Protective Domain Name System Resolver Service," *Cybersecurity & Infrastructure Security Agency (US)*, https://www.cisa.gov/sites/default/files/publications/PDNS%20Fact%20Sheet%20Updated_508c.pdf.

⁸⁷ "Name Collision Analysis Project Study Two Report," April 5, 2024, <https://www.icann.org/en/system/files/files/ncap-study-2-report-05apr24-en.pdf>.

6.4 Blockchain-Based Domains

A number of alternative name resolution protocols have been proposed, many of these utilizing blockchains or public ledgers.^{88,89,90} Many of these are specifically designed to be "censorship resistant," both in terms of blocking resolution, as well as in terms of the ability to seize or alter the target of the names. An example is the GNU Naming System (GNS).⁹¹

The majority of these systems use names which are syntactically identical to DNS names, but do not use the DNS for resolution. This means that attempting to block these names in the DNS will not accomplish anything on the blockchain. By design, many of these systems do not have a mechanism for the name system provider to override or change resolution of names within the system, which means that the provider cannot be compelled to remove a name.

The SSAC report on the evolution of Internet name resolution discusses the permanence of names in the DNS and in blockchain. SAC123 states: "Censorship resistance is another motivation of some experimenters. Websites and [DNS] domain names can be taken down by any of several parties: the registrar, the registry, the nameserver operator, or the hosting company. This has led to technologies that promise different levels of permanence in naming and that can make the promise that once a name has been added to the system it cannot be removed. This, in turn, has motivated different kinds of distributed ledgers, such as blockchains, to be developed and deployed that can provide different assurances of permanence."⁹²

6.5 Encrypted DNS: DoH, DoT, and DoQ (Collectively, DoX)

In recent years, the DNS has seen the deployment of various encryption mechanisms designed to safeguard both DNS queries and responses. These innovations aim to enhance user privacy and security by encrypting DNS traffic, both between the client and resolver, as well as eventually between recursive resolvers and authoritative resolvers, so that they cannot be easily intercepted, read, or altered by third parties during transmission.

⁸⁸ ICANN Security and Stability Advisory Committee (SSAC), "SAC123 – SSAC Report on the Evolution of Internet Name Resolution," Dec 15, 2023, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-123-15-12-2023-en.pdf>.

⁸⁹ Paul Hoffman, ICANN Office of the Chief Technology Officer, "OCTO-039: Introduction to Blockchain Name System Technologies," Oct 17, 2024, <https://www.icann.org/en/system/files/files/octo-039-17oct24-en.pdf>.

⁹⁰ Paul Hoffman, ICANN Office of the Chief Technology Officer, "OCTO-040: Introduction to Blockchain Technologies," Oct 17, 2024, <https://www.icann.org/en/system/files/files/octo-040-17oct24-en.pdf>.

⁹¹ Matthias Wachs, Martin Schanzenbach, and Christian Grothoff. "A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System." In *Cryptology and Network Security*, edited by Dimitris Gritzalis, Aggelos Kiayias, and Ioannis Askoxylakis, 127–42. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2014. https://doi.org/10.1007/978-3-319-12280-9_9.

⁹² ICANN Security and Stability Advisory Committee (SSAC), "SAC123 – SSAC Report on the Evolution of Internet Name Resolution," Dec 15, 2023, p. 15, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-123-15-12-2023-en.pdf>.

These mechanisms are:

- **DoH:** RFC8484 - "DNS Queries over HTTPS (DoH)." This protocol routes DNS queries and responses over the encrypted HTTPS protocol, typically used for secure web browsing. By leveraging existing HTTPS infrastructure, DoH effectively camouflages DNS traffic as regular web traffic, making it difficult to distinguish and block.⁹³
- **DoT:** RFC7858 - "Specification for DNS over Transport Layer Security (TLS)." DNS-over-TLS (DoT) establishes a secure, encrypted tunnel specifically for DNS communication over the Transport Layer Security (TLS) protocol. This ensures the confidentiality and integrity of DNS data while in transit.⁹⁴
- **DoQ:** RFC9250 - "DNS over Dedicated QUIC Connections." DNS-over-QUIC (DoQ) utilizes the QUIC protocol, a modern transport protocol known for its speed and security enhancements. By encrypting DNS traffic over QUIC, DoQ offers improved performance and resistance to network interference.⁹⁵

The adoption of these encryption mechanisms (collectively called DoX) has had significant implications for user privacy and security, as well as for entities attempting to block or filter DNS queries. DoX effectively "hides" DNS traffic within the encrypted flow of web traffic, making it nearly indistinguishable from regular web browsing activity. This presents a challenge for network administrators, ISPs, governments, schools, or workplaces that may wish to enforce content restrictions or monitor online activities through DNS filtering. Traditional methods of content filtering or network monitoring that rely on identifying and manipulating DNS requests become ineffective when faced with the encrypted and obfuscated nature of DoX traffic.⁹⁶

The technical intricacies of DoX make it difficult to differentiate DNS traffic from other HTTPS or QUIC traffic without deep packet inspection (DPI). While DPI can be employed to identify DoX traffic, it is a resource-intensive process that raises privacy concerns and may not be feasible for all networks.

In one study, blocking focused on preventing Transmission Control Protocol (TCP) or TLS communication between a probe system and the IP address(es) used by DoT/DoH services.⁹⁷ A previous SSAC report discussed the implications of DNS encrypted transport in applications,

⁹³ "RFC 8484: DNS Queries over HTTPS (DoH)," *Internet Engineering Task Force (IETF)*, January 15, 2019, <https://datatracker.ietf.org/doc/rfc8484/>.

⁹⁴ "RFC 7858: Specification for DNS over Transport Layer Security (TLS)," *IETF*, December 20, 2018, <https://datatracker.ietf.org/doc/rfc7858/>.

⁹⁵ "RFC 9250: DNS over Dedicated QUIC Connections," *IETF*, April 24, 2024, <https://datatracker.ietf.org/doc/rfc9250/>.

⁹⁶ See footnote 19 at: "Compliance and Enforcement and Telecom Decision CRTC 2022-170," *Canadian Radio-television and Telecommunications Commission*, June 23, 2022, <https://crtc.gc.ca/eng/archive/2022/2022-170.htm>.

⁹⁷ Simone Basso, "Measuring DoT/DoH Blocking Using OONI Probe: A Preliminary Study," *Open Observatory of Network Interference (OOONI)*, June 17, 2022, <https://ooni.org/post/2022-doh-dot-paper-dnsprivacy21/>.

examining DNS over HTTPS and DNS over TLS, which describes the topic in a greater level of technical detail.⁹⁸

6.6 Extended DNS Error

Traditionally, DNS errors have been cryptic and lacked transparency, leaving users with little information about the reasons behind failed domain resolutions. RFC 8914:Extended DNS Errors introduces a notable enhancement to the DNS by enabling blocking resolvers to provide more informative error codes and communicate the nature of the blocking.⁹⁹ One such code is "Extended DNS Error Code 16 - Censored," which serves as a clear signal to users that their attempted access to a specific domain has been intentionally blocked by a deliberate action taken by an external entity, distinct from the DNS resolver or forwarder.

For example, Google Public DNS provides a query response that returns REFUSED with an extended DNS error 16 ("Censored").¹⁰⁰

The "Censored" error code, in particular, serves as a powerful tool for user empowerment. It explicitly reveals that the block is not arbitrary but instead results from an external requirement. The "Censored" error code allows users to investigate the reasons behind the block, contact the responsible entity to inquire about their policies, or explore alternative means of accessing the desired content.

Furthermore, this enhanced error reporting promotes accountability and transparency. By explicitly identifying the block as externally imposed, it places the responsibility on the appropriate entity, whether it be a government agency, ISP, or other organization. This transparency can deter overblocking and encourage a more measured approach to content filtering.

There is related work underway in the Internet Engineering Task Force (IETF) to allow more clear signalling of when DNS blocking is occurring. An IETF draft notes that "filtered DNS responses lack structured information for end users to understand the reason for the filtering. Users of DNS services that perform filtering may wish to receive more explanatory information about such a filtering to resolve problems with the filter."¹⁰¹ We look forward to the technical community developing and deploying Request for Comments (RFC)s and best practices related to the

⁹⁸ ICANN Security and Stability Advisory Committee (SSAC), "SAC109: The Implications of DNS over HTTPS and DNS over TLS," March 12, 2020, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-109-en.pdf>.

⁹⁹ Warren Kumari, et.al. "RFC 8914 – Extended DNS Errors," *Internet Engineering Task Force*, October 23, 2020. <https://datatracker.ietf.org/doc/rfc8914/>.

¹⁰⁰ "Blocking Behavior," *Google Public DNS*, September 3, 2024, <https://developers.google.com/speed/public-dns/blocking>

¹⁰¹ Internet Engineering Task Force, "Structured Error Data for Filtered DNS," (draft-ietf-dnsop-structured-dns-error-10) <https://datatracker.ietf.org/doc/draft-ietf-dnsop-structured-dns-error/>

implementation of such signalling, which can be used to provide more clear indications of DNS blocking to end users and troubleshooters.

7 Recommendations

Recommendation 1: SSAC recommends that any entity implementing or mandating DNS blocking understand the implications of the technology.

Recommendation 2: SSAC recommends that DNS blocking implemented by any entity—by a government or any organization that has policy, legal, or operational control over a network or service—follow these guidelines:

- A. The entity should determine whether DNS blocking will fulfill its objectives.
- B. The entity should have a clear policy about what and how it will block, with well-defined review and decision-making processes that minimize risk.
- C. The entity should implement the policy using a technique that minimizes overblocking or collateral damage that could affect its users.
- D. The entity should not affect networks or users outside its administrative control.

Recommendation 3: SSAC recommends that operators of recursive servers use DNS Extended Error codes (see section [6.6 Extended DNS Error](#)) to indicate to end users and troubleshooters that DNS blocking is taking place.

8 Acknowledgments, Disclosures of Interest, and Withdrawals

In the interest of transparency, these sections provide the reader with information about aspects of the SSAC process. The Acknowledgements section lists the SSAC members, outside experts, and ICANN staff who co-authored or contributed directly to this particular document or who provided reviews. The Disclosures of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this report. The Withdrawals section identifies individuals who have recused themselves from the discussion of the topic with which this report is concerned. Except for members listed in the Withdrawals section, this document has the consensus approval of all of the members of SSAC.

8.1 Acknowledgments

The committee wishes to thank the following SSAC members, invited guests, and ICANN staff for their time, contributions, and review in producing this report.

SSAC Members

Greg Aaron (work party co-chair)
Joe Abley
Benedict Addis
Maarten Aertsen
Gautam Akiwate
Tim April
Jeff Bedser
Lyman Chapin
KC Claffy
Patrik Fältström (SSAC Member through 31 December 2024)
James Galvin
Robert Guerra
Russ Housley
Matthias Hudobnik
Geoff Huston
Merike Kão (SSAC Member through 31 December 2024)
Andrey Kolesnikov
Warren “Ace” Kumari (work party co-chair)
Barry Leiba
John Levine
Hadia el Miniawi
Ram Mohan
Rod Rasmussen
Matthew Thomas
Peter Thomassen
Rick Wilhelm

Invited Guests

Merike Kão (Invited Guest after 1 January 2025)

ICANN Staff

John Emery (editor)
John Kristoff
Michael Puckett
Carlos Reyes
Danielle Rutherford
Kathy Schnitt
Steve Sheng (SSAC Support Staff through 30 November 2024)
Samaneh Tajalizadehkhoob

8.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest at the time of publication are available at: <https://www.icann.org/en/ssac/members/archive/16-05-2025>.

8.3 Withdrawals

There were no withdrawals.