ISOC Perspectives on Domain Name System (DNS) Filtering
August/2011

Issue: Finding Solutions to Illegal On-line Activities

Policymakers, legislators, and regulators around the globe want to combat illegal online activities such as child pornography, infringement of intellectual property rights and cybercriminal activities.

"DNS filtering" is one of the solutions currently in use. DNS filtering requires Internet Service Providers to change Domain Name System (DNS) information passing through their networks, redirecting to a different site than the one intended by the Internet user. The goal of DNS filtering is to block access to web sites that have been determined to be distributing illegal content. An alternative to DNS filtering is domain name seizure or domain blocking, a non-technical approach where a national authority could order that a domain name be changed or entirely removed from the global DNS.[1]

The Internet Society believes that DNS filtering and domain name seizure do not solve the problem and undermine the Internet as a single, unified, global communications network. DNS filtering and seizure also raise concerns with regard to human rights, freedom of expression, and the free flow of information, as well as the respect of basic rule of law and due process principles.

ISOC recognizes that policy makers have an important obligation to address online cybercrime and illegal online content, but we encourage technical and policy collaboration to identify solutions based on international cooperation that do not harm the global DNS infrastructure.

Background

The most effective way to combat illegal online activities such as dissemination of child pornography is to attack them at their source. For example, a suitable national authority within a country could order that a server in that country with illegal content be removed from the Internet.[2]

However, in the multi-national environment of the Internet, stopping the source of illegal content is more complicated than simply shutting down a local server. Often, the person providing the content, the servers hosting the content, and the domain name pointing to the content are in three different countries, all beyond the jurisdiction of an individual national regulator. The international element is further complicated by differing laws covering what is and what is not "illegal content," especially in the areas of free speech[3] and intellectual property protection.

An alternative approach to blocking the source of illegal content has been to interfere with the consumption of the content. When the national regulator is in the same jurisdiction as the consumer, blocking consumption seems to offer an appealing way around the complexities and overhead of cross-border actions.

DNS filtering has been proposed as a way to block content consumption. The Domain Name System (DNS) is a global database that translates domain names (such as

---

[1] For example, the isoc.de (German chapter of ISOC) name is held at the German national ".DE" registrar, and a suitable authority within Europe could order the registrar to remove the name, making it completely unavailable to the entire Internet. The non-country domain names (those ending in .COM, .NET, and .ORG for example) are more complicated to deal with since they are implicitly multi-national, although *de facto* firmly within US controls, with the resulting jurisdictional difficulties.

[2] If the server has both legal and illegal content, this raises additional concerns.

[3] For example, in Germany, a web page with a swastika may be considered illegal, while the same web page could be protected speech in neighboring France. In Beijing, a web page critical of the Communist Party may be considered seditious, while the same content could be considered patriotic in neighboring Taipei.

www.isoc.org) to Internet addresses that are used by computers to communicate. When any Internet user types or clicks on a domain name in a web browser, the name must be translated into an Internet address first before the page can be displayed.

This translation is required by the underlying protocols of the Internet. Every Internet-connected device, whether a laptop computer, smart phone, or gaming console, must lookup each name in the global DNS, and then use the resulting Internet addresses to connect to the web server. This lookup and translation are transparent to the user, but are critical to the successful operation of the Internet.

All traffic from an Internet user passes through their Internet Service Provider (ISP), making the ISP a target for implementing DNS filtering, in order to block the consumption of illegal content.[4] DNS filtering requires the ISP to intercept, inspect, and potentially modify the results of each customer's DNS lookups. When a prohibited web site is identified, a response is sent either to indicate an error, or to direct the user to some other location, such as a web page indicating that access has been blocked.

DNS filtering can be enforced by the local ISP, or at the national level.[5] The key characteristic of DNS filtering is that DNS responses are modified as they pass through the network, making them different from the original data published in the global DNS. The modifications take place without the knowledge or consent of the end user.

Negative Consequences of DNS Filtering

DNS filtering has technical drawbacks, potential human rights and due process issues, as well as long-term consequences for the stability and interoperability of the Internet. Because DNS filtering modifies the operation of the DNS, a fundamental building block of the Internet, it will have long-term effects that reduce the reliability, openness, and usability of the global Internet.[6]

Problem	Details
Easily circumvented	Users who wish to download filtered content can simply use IP addresses instead of DNS names. As users discover the many ways to work around DNS filtering, the effectiveness of filtering will be reduced. ISPs will be required to implement stronger controls, creating an unwelcome escalating war between Internet users and their trusted service providers and national governments.
Doesn't solve the problem	Filtering DNS or blocking the name does not remove the illegal content. A different domain name pointing to the same Internet address could be established within minutes.
Incompatible with DNSSEC	DNSSEC, a new technology designed to add confidence and trust to DNS, ensures that DNS data are not modified by malicious third parties between the data owner and the consumer. To DNSSEC, DNS filtering looks the same as a hacker trying to impersonate a legitimate web site to steal personal information—exactly the problem that DNSSEC is trying to solve.
Puts users at-risk	When local DNS service is not considered reliable and open, Internet users may use alternative and non-standard approaches, such as downloading software that redirects their traffic to avoid filters, which subjects them to additional security risks.
Encourages fragmentation	A coherent and consistent structure is important to the successful operation of the Internet. DNS filtering eliminates this consistency and fragments the DNS, which undermines the structure of the Internet.

[4] DNS filtering is most effective in blocking access to content on web servers. DNS filtering is **not** effective in blocking other content distribution methods, such as peer-to-peer networks that make minimal or no use of DNS.

[5] Internet Service Providers are the normal place for DNS filtering to be enforced, but in the case of countries with a small number of known Internet connections, a national authority with control over all connections could also execute the filtering operation for the entire country, or in a specific region.

[6] These issues are discussed in detail in the "... Technical Concerns Raised by the DNS Filtering ..." paper cited below.

Drives service underground	If DNS filtering becomes widespread, "underground" DNS services and alternative domain hierarchies will be established, further fragmenting the Internet, and taking the content out of easy view of law enforcement.
Raises privacy concerns	ISPs have always been able to inspect and log DNS traffic through their networks. DNS filtering, however, raises the spectre of an ISP "spying" on their customers and reporting on the contents of their DNS queries.
Raises human rights and due process concerns	DNS filtering is a broad measure, unable to distinguish illegal and legitimate content on the same server. Implemented carelessly or improperly, it has the potential to cause significant collateral damage and restrict free and open communications.

ISOC position: Talking Points and Conclusions

DNS is one of the fundamental protocols on which overall global Internet functionality is built**.** DNS filtering causes instability, encourages fragmentation, and undermines the foundation of the Internet. Domain name seizure suffers from most of the same problems as DNS filtering, including easy circumvention, failure to solve the underlying problem, and encouragement of a shadow network out of reach of law enforcement.

Unilateral modification of DNS behavior carries high risks. As detailed in the table above, DNS filtering is incompatible with DNSSEC, reducing global Internet security; DNS filtering encourages the creation of alternative non-standard DNS systems, putting individual users at risk. Because almost every system and service in the Internet depends on DNS, filtering will affect more users than are intended. Filtering creates a highly fragmented, country-by-country Internet rather than one global network. What is filtered in Pakistan may affect users in Panama. *Filtering the global DNS has risks to users and will decrease global security.*

Filtering DNS does not solve the problem. Changing the DNS doesn't remove the objectionable or illegal content from the Internet; it simply makes it harder to get to. Users who are determined to download this type of material will still be able to do so. If DNS filtering is used in many countries, then these users will also set up "shadow" Internet structures to avoid filtering, making it more difficult for law enforcement to observe and intervene. *Policy makers should focus on the most effective ways to solve the problem.*

Filtering DNS causes significant collateral damage. We already have abundant anecdotal evidence that DNS filtering will affect users and content providers engaging in completely legal activities. For example, in February 2011, US authorities blocked the domain "mooo.com," because some child pornography was found on a sub-domain. The blockage also affected over 80,000 other (presumably legal) web sites set up as sub-domains of mooo.com. This collateral damage could be minimized by very careful technical implementation, but it can never be eliminated.[7] *The cost of DNS filtering outweighs possible short-term benefits.*

DNS filtering has non-technical side effects. The fundamental problem is a non-technical problem: how to keep illegal content off of the Internet. Solving this non-technical problem with technology, such as DNS filtering, raises privacy and public policy issues. Basic principles of the rule of law, such as the presumption of innocence until proven guilty and other questions such as due process have not been well

[7] Because of the way DNS was designed, domain names map poorly to individuals or organizations. DNS names act much like physical property: it's easy to look up the listed owner of a lot or building, but much more difficult to tell who that owner really is, or whether they are occupying the property, sub-leasing it, or have established a multi-tenant facility.

addressed by proposed legislation calling for DNS filtering. *"Quick and easy" technical solutions to non-technical problems need to be considered as carefully as any other legislation to avoid human rights-related side effects.*

International cooperation is the real solution. These are cross-border issues and will not be effectively solved on a country-by-country basis. This should be taken up on an international level as part of a continuing dialogue between regulators and the Internet community. For example, better authentication of DNS name registrants internationally which would allow for the possibility of tracking back bad behavior to an identifiable person, which itself may act as a deterrent. Other levers, such as attacking the payment systems used by cyber-criminals, may also yield longer-lasting and more effective results. *International cooperation provides the structure that policymakers need to solve this problem.*

Additional Resources

The resources in this section may be helpful in understanding the context for DNS filtering, as well as alternative views on the legal, technical, and security implications of DNS filtering and domain name seizure.

S. 968: "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011" GovTrack.
http://www.govtrack.us/congress/bill.xpd?bill=s112-968

Professors' Letter in Opposition to "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011" (PROTECT-IP Act of 2011, S. 968), July 5, 2011.
http://blogs.law.stanford.edu/newsfeed/files/2011/07/PROTECT-IP-letter-final.pdf

SAC 050: 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
http://www.icann.org/en/committees/security/sac050.pdf

Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill
http://www.shinkuro.com/PROTECT%20IP%20Technical%20Whitepaper%20Final.pdf

About the Internet Society

The Internet Society (ISOC) is a non-profit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. With more than 100 organizational and 50,000 individual members, we are the largest public organization focusing on the Internet. ISOC is the organizational home of the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB), responsible for the technical standards and design of the Internet. We are dedicated to ensuring the open development, evolution and use of the Internet for the benefit of people throughout the world.