Internet Society Perspectives on Domain Name System (DNS) Filtering:

Filtering is not a solution - the real solution is international cooperation

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. The Internet Society agrees that these are critical issues to address but we also believe that they must be in ways that do not undermine the global architecture of the Internet or curtail internationally recognized human rights.

The most effective way to combat illegal online activities such as dissemination of child pornography is to attack them at their source. The multi-national environment of the Internet, however, makes stopping the source of illegal content more complicated than simply shutting down a local server. The different actors involved in delivering the source's content to consumers may be in different countries, with different laws covering what is and is not "illegal content". Thus, the alternative approach of interfering with the consumption of the content is sometimes suggested. When the national authority is in the same jurisdiction as the consumer of content, blocking consumption seems an easy way around the complexities and overhead of cross-border actions. To that end, national authorities have proposed the implementation of DNS filtering as a way to address content perceived to be illegal within their jurisdiction.

The Internet Society believes that policies and regulations that require the interruption of the DNS infrastructure, whether by filtering results or through domain name seizure[1], have serious deficiencies. These techniques do not solve the problem, interfere with cross-border data flows and services, and undermine the Internet as a single, unified, global communications network. DNS filtering and seizure raise human rights and freedom of expression concerns, and often curtail international principles of rule of law and due process. The negative impact of DNS filtering far outweighs the short-term legal and business benefits.

ISOC recognizes that policy makers have an important obligation to address online cybercrime and illegal online content. We encourage technical and policy collaboration to identify solutions based on international cooperation that do not harm the global DNS infrastructure or the overall stability and interoperability of the Internet.

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

[1] An alternative to DNS filtering is domain name seizure, a non-technical approach where a national authority could order that a domain name be changed or entirely removed from the global DNS. 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.

be removed from the Internet.[2]

The multi-national environment of the Internet, however, makes stopping the source of illegal content 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 authority. Each of the countries involved may have differing laws covering what is and is not "illegal content," especially in the areas of free speech and intellectual property protection.[3]

An alternative approach to blocking the source of illegal content has been to interfere with the consumption of the content. When the national authority is in the same jurisdiction as the consumer, blocking consumption seems an easy 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 www.example.com) 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.

Use of domain names is a fundamental part of the Internet. Every Internet-connected device, whether a personal computer, smart phone, or gaming console, looks up each name in the global DNS, and uses the resulting Internet address to connect to the web server, send the e-mail or use the application. The lookup and translation are transparent to the user, and 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 an appealing point for DNS filtering 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.[5] When a prohibited web site is looked up, the filtered result sent to the user either indicates the site doesn't exist, or directs the user to another site, such as a web page saying access has been blocked.

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

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

[3] For example, in March, 2011, the domain name "rojadirecta.org" owned by a Spanish company was seized by US authorities under a US warrant, even though a Spanish court had found the web site was operating legally. This example also highlights the complexity of seizure of non-country domain names (those ending in .COM, .NET, and .ORG for example) which are implicitly multi-national, although *de facto* firmly within control of whichever country houses the registrar for the non-country domain.

[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] DNS filtering an be enforced by the ISP or at the ational level. ISPs 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 implement the filtering operation for the entire country, or in a specific region.

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, placing them in the middle of an unwelcome battle between Internet users 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 and impedes DNSSEC deployment	DNSSEC is a new technology designed to add confidence and trust to the Internet. DNSSEC ensures that DNS data are not modified by anyone 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. DNSSEC cannot differentiate legally sanctioned filtering from cybercrime.
Causes collateral damage	When both legal and illegal content share the same domain name, DNS filtering blocks access to everything. For example, blocking access to a single Wikipedia article using DNS filtering would also block millions of other Wikipedia articles.
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. These makeshift solutions subject users 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.
Drives service underground	If DNS filtering becomes widespread, "underground" DNS services and alternative domain namespaces will be established, further fragmenting the Internet, and taking the content out of easy view of law enforcement.
Raises human rights and due process concerns	DNS filtering is a broad measure, unable to distinguish illegal and legitimate content on the same domain. Implemented carelessly or improperly, it has the potential to restrict free and open communications and could be used in ways that limit the rights of individuals or minority groups.

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

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

objectionable or illegal content from the Internet; it makes it simply 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 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 have abundant anecdotal evidence that DNS filtering will affect users and content providers engaging in completely legal activities. For example, in February 2011, U.S. authorities blocked the domain "mooo.com," because some child pornography was found on a sub-domain. The blockage also affected over 80,000 other legal web sites set up as sub-domains of mooo.com. In some cases, collateral damage can 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 implications. The fundamental issue is non-technical: 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. DNS filtering erodes trust in the Internet when users are no longer certain that typing www.isoc.org into a web browser will get them to the ISOC web site. To address the issues of illegal online activities, policy makers need to act in accordance with basic international norms including the rule of law and standards of due process. *"Quick and easy" technical solutions to non-technical problems must be considered carefully to avoid infringing internationally-agreed human rights and eroding trust in the Internet.*

The real solution to combating illegal activities is to attack them at the source, through international cooperation. These are cross-border issues and cannot be effectively solved on a country-by-country basis. A continuing dialogue between national authorities and the Internet community can help. For example, better authentication of DNS name registrants 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 appropriate avenue for policymakers and the technical community to solve this problem.*

Additional Resources
The resources in this section provide background information, and offer context and alternative views on the legal, technical, and security implications of DNS filtering and domain name seizure.

"The Internet Domain Name System Explained for Non-Experts" (ISOC Briefing provided by Daniel Karrenberg), February, 2004.
http://www.isoc.org/briefings/016/

S. 968: "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011," available via 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.

[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.

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-partisan, non-profit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. With more than 100 organizational and 44,000 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.