Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill

May 2011

Authors: Steve Crocker, Shinkuro, Inc.
David Dagon, Georgia Tech
Dan Kaminsky, DKH
Danny McPherson, Verisign, Inc.
Paul Vixie, Internet Systems Consortium

Affiliations provided for identification only
Brief biographies of authors available below

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This paper describes technical problems raised by the DNS filtering requirements in S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 ("PROTECT IP Act"). Its authors come from the technical, operational, academic, and research communities. We are leading domain name system (DNS) designers, operators, and researchers, who have created numerous "RFCs" (technical design documents) for DNS, published many peer-reviewed academic studies relating to architecture and security of the DNS, and operate important DNS infrastructure on the Internet.

The authors of this paper take no issue with strong enforcement of intellectual property rights generally. The DNS filtering requirements in the PROTECT IP Act, however, raise serious technical concerns, including:

- The U.S. Government and private industry have identified Internet security and stability as a key part of a wider cyber security strategy, and if implemented, the DNS related provisions of PROTECT IP would weaken this important commitment.
- DNS filters would be evaded easily, and would likely prove ineffective at reducing online infringement. Further, widespread circumvention would threaten the security and stability of the global DNS.
- The DNS provisions would undermine the universality of domain names, which has been one of the key enablers of the innovation, economic growth, and improvements in communications and information access unleashed by the global Internet.
- Migration away from ISP-provided DNS servers would harm efforts that rely on DNS data to detect and mitigate security threats and improve network performance.
- Dependencies within the DNS would pose significant risk of collateral damage, with filtering of one domain potentially affecting users' ability to reach non-infringing Internet content.
- The site redirection envisioned in Section 3(d)(II)(A)(ii) is inconsistent with security extensions to the DNS that are known as DNSSEC. The U.S. Government and private industry have identified DNSSEC as a key part of a wider cyber security strategy, and many private, military, and governmental networks have invested in DNSSEC technologies.
- If implemented, this section of the PROTECT IP Act would weaken this important effort to improve Internet security. It would enshrine and institutionalize the very network manipulation that DNSSEC must fight in order to prevent cyberattacks and other malevolent behavior on the global Internet, thereby exposing networks and users to increased security and privacy risks.

We believe the goals of PROTECT IP are important, and can be accomplished without reducing DNS security and stability through strategies such as the non-DNS remedies contained in PROTECT IP and international cooperation.

I. Introduction

The recently introduced PROTECT IP Act of 2011,[1] the successor to last year's COICA legislation,[2] includes a range of proposed new enforcement mechanisms to combat the online infringement of intellectual property. Of keen interest to the community of engineers working on issues related to the domain-name system (DNS) is the DNS filtering provision that would require ISPs and other operators of "non-authoritative DNS servers" to take steps to filter and redirect requests for domains found by courts to point to sites that are dedicated to infringement. This paper seeks to explain a set of technical concerns with mandated DNS filtering and to urge lawmakers to reconsider enacting such a mandate into law.

Combating online infringement of intellectual property is without question an important objective. The authors of this paper take no issue with the lawful removal of infringing content from Internet hosts with due process. But while we support the goals of the bill, we believe that the use of mandated DNS filtering to combat online infringement raises serious technical and security concerns.

Mandated DNS filtering would be minimally effective and would present technical challenges that could frustrate important security initiatives. Additionally, it would promote development of techniques and software that circumvent use of the DNS. These actions would threaten the DNS's ability to provide universal naming, a primary source of the Internet's value as a single, unified, global communications network.

II. DNS Background

The domain-name system, or DNS, is a system that makes the Internet more accessible to humans. When computers on the Internet communicate with each other, they use a series of numbers called "IP addresses" (such as 156.33.195.33) to direct their messages to the correct recipient. These numbers, however, are hard to remember, so the DNS system allows humans to use easier-to-remember words (such as "senate.gov") to access websites or send e-mail. Such names resolve to the proper IP numbers through the use of domain name servers. These servers are set up in a distributed fashion, often globally, such that resolution of names connected to IP addresses may pass through many servers during Internet data flow.[3] To make the DNS faster and less expensive to operate, over ten million so-called "recursive servers" exist as accelerators of convenience, to store and retransmit DNS data to nearby users. The PROTECT IP Act proposes legal remedies for infringement that would affect the operators of these "recursive

[1] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Congress

[2] Combatting Online Infringements and Counterfeits Act, S. 3480, 111th Congress

[3] *See* P. Mockapetris, RFC 1034, "Domain Names – Concepts and Facilities," Internet Engineering Task Force, November 1987, http://www.ietf.org/rfc/rfc1034.txt.

servers," which are the type of DNS servers used by the computers of end users to resolve DNS names in order to access content on the Internet.[4]

The DNS is central to the operation, usability, and scalability of the Internet; almost every other protocol relies on DNS resolution to operate correctly. It is among a handful of protocols that that are the core upon which the Internet is built. Readers interested in finding out more about the DNS are directed to Paul Vixie's article, "DNS Complexity."[5] See also Appendix A for a pictorial view of the DNS and DNS filtering.

The DNS is a crucial element of Internet communication in part because it allows for "universal naming" of Internet resources. Domain names have in almost all cases been universal, such that a given domain name means the same thing, and is uniformly accessible, no matter from which network or country it is looked up or from which type of device it is accessed.

This universality is assumed by many Internet applications. The domain name given to an Internet device or service is frequently stored and reused, or forwarded to other Internet devices that may not be customers of the same service provider or residents in the same country. For example, web URLs are frequently sent inside electronic mail messages where they are expected to mean the same thing (*i.e.*, to reach the same content) to the recipient of the e-mail that they meant to the sender. Universality of domain names has been one of the key enablers of the innovation, economic growth, and improvements in communications and information access unleashed by the global Internet. The importance of universal naming is underscored in the U.S. International Strategy for Cyberspace: "The United States supports an Internet with end-to-end interoperability, which allows people worldwide to connect to knowledge, ideas, and one another through technology that meets their needs."[6]

Mandated DNS filtering by nameservers threatens universal naming by requiring that some nameservers return different results than others for certain domains. While this type of mandated DNS manipulation is reportedly used in some Middle Eastern countries and in the so-called Great Firewall of China, the mandated DNS filtering proposed by PROTECT IP would be unprecedented in the United States and poses some serious concerns as described below.

[4] The other type of DNS server is termed "authoritative." These systems are the DNS servers that are usually under control of the content provider, and that provide the "authoritative" answer as to where on the Internet a given website or service is located. Essentially, "recursive" servers are the DNS servers that help users locate where things are on the Internet, and "authoritative" servers are the DNS servers are the sources of the answers to those queries. Because the focus of the PROTECT IP Act is on recursive DNS servers (and not authoritative servers), the terms "server," and "DNS server," and "resolver" in the remainder of this paper shall mean recursive servers that help users locate content and services on the Internet.

[5] Paul Vixie, "DNS Complexity," *ACM Queue 5*, no. 3, April 2007.

[6] United States Office of the President, *International Strategy for Cyberspace*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, at page 8.

III. Technical Challenges Raised By Mandatory DNS Filtering

A. DNS Filtering in Tension with DNSSEC

PROTECT IP would empower the Department of Justice, with a court order, to require operators of DNS servers to take steps to filter resolution of queries for certain names. Further, the bill directs the Attorney General to develop a textual notice to which users who attempt to navigate to these names will be redirected.[7] Redirecting users to a resource that does not match what they requested, however, is incompatible with end-to-end implementations of DNS Security Extensions (DNSSEC), a critical set of security updates. Implementing both end-to-end DNSSEC and PROTECT IP redirection orders simply would not work. Moreover, *any* filtering by nameservers, even without redirection, will pose security challenges, as there will be no mechanism to distinguish court-ordered lookup failure from temporary system failure, or even from failure caused by attackers or hostile networks.

Security problems with the DNS were identified over twenty years ago, and the DNSSEC approach to correcting vulnerabilities has been under development since the mid-1990s.[8] In short, DNSSEC allows for DNS records to be cryptographically signed, thereby providing a secure authentication of Internet assets. When implemented end-to-end between authoritative nameservers and requesting applications, DNSSEC prevents man-in-the-middle attacks on DNS queries by allowing for provable authenticity of DNS records and provable inauthenticity of forged data. This secure authentication is critical for combatting the distribution of malware and other problematic Internet behavior. Authentication flaws, including in the DNS, expose personal information, credit card data, e-mails, documents, stock data, and other sensitive information, and represent one of the primary techniques by which hackers break into and harm American assets.

DNSSEC has been promoted and supported by the highest levels of the U.S. government. Development and rollout has involved a major bipartisan political effort, undertaken at great expense as a public/private partnership dating back to the Clinton administration. President George W. Bush included securing the DNS among national cybersecurity priorities as early as 2003.[9] When the root zone trust anchor was published just under a year ago, enabling use of DNSSEC within the global DNS, the Obama administration hailed it as a "major milestone for Internet security."[10] The security of the Internet and the success of DNSSEC have been, and remain, a vital policy goal of the United States.[11]

[7] Section 3(d)(2)(A)(ii), "Text of Notice."

[8] *See* http://www.dnssec.net.

[9] United States Office of the President, *The National Strategy to Secure Cyberspace*, February 2003, *http*://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

[10] Andrew McLaughlin, "A Major Milestone for Internet Security," The White House blog, July 22, 2010, http://www.whitehouse.gov/blog/2010/07/22/a-major-milestone-internet-security.

[11] *See* United States Office of the President, *National Strategy for Trusted Identities in Cyberspace*, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*; See also* United States Office of the President, *International Strategy for Cyberspace*, May 2011, *supra*, note 6, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

The fundamental architectural concept behind DNSSEC is that any information associated with a name must verifiably come from the owner of that name. For example, DNSSEC is designed to ensure that if a user requests the mail server for the U.S. Senate, the response is actually the legitimate server to communicate with to send e-mail to addresses within the senate.gov domain. The power of DNSSEC is that it provides a widely deployed and well managed infrastructure that allows only the Senate IT staff to manipulate the authoritative senate.gov nameserver, while only the House of Representative's IT staff can manipulate the authoritative house.gov nameserver.

By mandating redirection, PROTECT IP would require and legitimize the very behavior DNSSEC is designed to detect and suppress. Replacing responses with pointers to other resources, as PROTECT IP would require, is fundamentally incompatible with end-to-end DNSSEC. Quite simply, a DNSSEC-enabled browser or other application cannot accept an unsigned response; doing so would defeat the purpose of secure DNS. Consistent with DNSSEC, the nameserver charged with retrieving responses to a user's DNSSEC queries cannot sign any alternate response in any manner that would enable it to validate a query.

Although DNSSEC-enabled applications are not yet in widespread use, the need for such applications has been a key factor driving DNSSEC's development. Today, applications and services that require security (*e.g.* online banking) rely on other forms of authentication to work around a potentially insecure DNS, but a secure DNS would be more effective and efficient. End-to-end deployment of DNSSEC is required to better secure the sensitive applications we have today and allow for new sensitive applications. A legal mandate to operate DNS servers in a manner inconsistent with end-to-end DNSSEC would therefore interfere with the rollout of this critical security technology and stifle this emerging platform for innovation.

Even DNS filtering that did not contemplate redirection would pose security challenges. The only possible DNSSEC-compliant response to a query for a domain that has been ordered to be filtered is for the lookup to fail. It cannot provide a false response pointing to another resource or indicate that the domain does not exist. From an operational standpoint, a resolution failure from a nameserver subject to a court order and from a hacked nameserver would be indistinguishable. Users running secure applications have a need to distinguish between policy-based failures and failures caused, for example, by the presence of an attack or a hostile network, or else downgrade attacks would likely be prolific.[12]

DNSSEC is being implemented to allow systems to demand verification of what they get from the DNS. PROTECT IP would not only require DNS responses that cannot deliver such proof, but it would enshrine and institutionalize the very network manipulation DNSSEC must fight in order to prevent cyberattacks and other miscreant behavior on the global Internet.

[12] If two or more levels of security exist in a system, an attacker will have the ability to force a "downgrade" move from a more secure system function or capability to a less secure function by making it appear as though some party in the transaction doesn't support the higher level of security. Forcing failure of DNSSEC requests is one way to effect this exploit, if the attacked system will then accept forged insecure DNS responses. To prevent downgrade attempts, systems must be able to distinguish between legitimate failure and malicious failure.

B. The Proposed DNS Filters Would Be Circumvented Easily

As described above, the DNS was adopted to achieve universal naming for Internet resources. The fact that host names resolve consistently regardless of which network performs the request is a key factor in the Internet's success as a global communications network. Anybody who has surfed to a site in a public place, an office, or someone else's house, and gone to a site different from what he or she is used to at home, will understand frustrations that can come from filtering. To the extent that the naming system becomes less universal or consistent, the economic and social value of the network will suffer.

DNS filtering does not remove or prevent access to Internet content. It simply prevents resolution by a particular DNS server of a filtered domain to its associated IP address. The offending site remains available and accessible through non-filtered nameservers or numerous other means, including direct accessibility from the client to the server if they have the corresponding information. Circumvention is possible, with increasing ease, and is quite likely in the case of attempts to filter infringement via the DNS. All of the methods that we discuss in this section pose risks to the security and stability of the DNS, and to broader societal concerns.

Evidence from the recent domain seizures by U.S. Immigrations and Customs Enforcement demonstrates how likely circumvention is to occur. Data captured by Arbor Networks regarding the seizure of TVShack.net, showed what appeared to be only a short term impact on actual traffic to the pirates' servers.[13] The content simply was moved to a different domain, with little long-term impact likely. Similarly, Alexa traffic rankings indicate that traffic to rojadirecta.es, the replacement for the seized rojadirecta.com, quickly reached levels comparable to that of the former domain.[14] This occurred due to the fact that users and infringing websites do not simply "give up" in response to implementation of a filtering mechanism. They go online, find new (non-American) domains or direct IP numbers, and connect as they usually would.

In the case of DNS filtering, users need not navigate to new domains, but can instead simply use non-filtered DNS servers. To understand this approach, it is helpful to understand what normally occurs for most residential broadband customer installations. Normally, as part of the initial settings provided by ISPs to their customers, the ISPs select the users' DNS server (commonly as part of dynamic addressing lease negotiation or in setting up a user's equipment). In general, the operator-selected DNS server is local to the user, providing fast, efficient resolution. Thus, for example, Comcast customers generally use Comcast's DNS servers allowing for an "accelerated," and topologically optimal, DNS experience.

However, users may change their DNS server settings, either by running a local resolver or by updating a single OS configuration parameter. Moreover, applications and even websites can also change a users' DNS settings automatically. A 2008 survey using data from Google found that hundreds of malware websites automatically change the DNS settings of users who simply

[13] Craig Labovtiz, "Takedown," Arbor Networks blog, July 2, 2010, http://asert.arbornetworks.com/2010/07/takedown/

[14] Compare http://www.alexa.com/siteinfo/rojadirecta.com# and http://www.alexa.com/siteinfo/rojadirecta.es#.

visit a malicious web site.[15] It is likely, if not inevitable, that infringement sites would use the same strategy, allowing a single site to instantly, silently, and permanently change a user's DNS path and evade DNS filtration and filtering.

How easily could software make such a change? Just a single line of code is needed to change one registry key in Microsoft Windows. As documented widely by Microsoft itself, software merely needs to edit one system registry parameter:

```
        \\HKLM\SYSTEM\CurrentControlSet\Services\DnsCache\Parameters
```
[16]

Such behavior is common. In a survey of 100,000 malware samples, pulled at random from the Georgia Institute of Technology's malware repository, over 98% were found to read Windows registry settings, and some 68% were found to change the registry. Indeed, the anti-malware industry even has a term for viruses that specifically manipulate resolution via registry keys: "DNS-changers", or "DNS-changing malware," and such techniques have been employed by miscreants for nearly a decade.[17]

The choice of alternative DNS servers is effectively unlimited. In the same study, a survey of so-called "open-recursive" DNS resolvers revealed a dramatic increase in the number of public DNS servers. At present, there are *tens of millions* of open, public DNS servers, many outside the U.S. Sites offering or promoting the downloading of copyright-infringing content could use almost any of these resolvers to evade domestic DNS filtering.

An obvious possibility would be for the operators of the infringement sites themselves to operate alternative DNS servers for their users. It has been suggested that perhaps pirate sites would not wish to operate such a service because it would be difficult or expensive. However, DNS resolvers are lightweight and do not expose the same network engineering profile or carry the same costs as other circumvention technologies such as full-traffic encryption. In practice, a $1,000 server can respond to over 100,000 DNS requests *per second*. It is substantially easier to provide the handful of bits required for a DNS response than to expose a complex searchable web interface to pirated content. Realistically, the DNS accelerating service could be provided at no additional cost, using spare capacity on existing servers. Thus, those entities large enough to attract the attention of PROTECT IP likely will be large enough to handle the DNS load of their user base.

Suggestions have been made that U.S. users will not use servers located outside of the United States because the nameservers are foreign and untrusted.[18] The user who is seeking pirated content, however, will often be more concerned about getting the content than with how reputable a particular DNS provider might be. More importantly, in many cases, the user will

[15] D. Dagon, N. Provos, C. P. Lee, and W. Lee, "Corrupted DNS resolution paths: The rise of a malicious resolution authority," In *Proceedings of Network and Distributed Security Symposium* (NDSS '08), 2008. Note: The 2008 study and this report share an author.

[16] Microsoft, Inc. DNS Registry Entries. http://technet.microsoft. com/en-us/library/dd197418%28WS.10%29.aspx, 2011.

[17] Dagon et. al., "Corrupted DNS resolution paths," *supra,* note 15; *see also* Symantec, Description of Trojan.Qhosts virus, http://www.symantec.com/security_response/writeup.jsp?docid=2003-100116-5901-99.

[18] Daniel Castro, "No, COICA Will Not Break the Internet," Innovation Policy blog, January 18, 2011, http://www.innovationpolicy.org/no-coica-will-not-break-the-internet.

likely have no idea that they are changing DNS servers. Those promoting pirate sites will simply create websites and postings that ask: "Frustrated by getting filtered when you try to watch movies? Click here to fix the problem." Long experience shows that high numbers of users will simply do just that; they will "click here" and thereby quickly circumvent the intended roadblock through automated processes such as DNS changers.

Would users care about performance? One theory states that users would avoid these non-U.S nameservers because they would be slower, if for no other reason that they are offshore and thus may take up to a substantial fraction of a second to return answers. There is some data that slower sites are slightly less popular, but it is unlikely that foreign DNS would slow things down enough, for a number of reasons.

First, the likely delay for a site would only be a few tenths of a second. Second, only the initial query to a domain is impacted. Third, most modern browsers implement something called DNS prefetching, performing the DNS lookup before the user even browses to a site. Consequently, users will likely not even experience the delay when navigating to a given site. Finally, from the perspective of a user seeking pirated content, a slightly slower site is much better than not being able to access the site and its infringing content at all.

However, even if one supposed that all malicious sites changing DNS settings were filtered, and even if one supposed that 100% of users leave their ISPs' DNS settings unchanged, mandatory DNS filtering still could be *trivially* evaded by individuals and even applications.

The IP number for the website of The Pirate Bay, a well-known peer-to-peer (P2P) organization that has often been connected to infringement allegations, is 194.71.107.15. Simply typing this number instead of www.piratebay.org into a browser's address line will take a user to the site. To avoid having to remember the number each time, PCs can easily be configured to bypass DNS filters.

Effectively, all systems have within them something called a hosts file, which is in text format. After simple editing of a hosts file with the additional line "www.thepiratebay.org 194.71.107.15", the DNS will no longer be consulted.

Many users will not have the expertise necessary to rewrite a host file. On the other hand, individuals who are skeptical of this potential for evasion should consider that software developers already are working on software to evade DNS filtration. A group calling itself "MafiaaFire" has developed a Firefox browser plugin that automatically redirects users requesting a seized domain to the desired site's new domain or server IP address.[19] (A screen image that shows the ease with which Internet users can implement such tools is in Appendix B). Infringers are almost certain to develop similar plugins that skip the DNS entirely, perhaps simply by putting links on their pages which offer to make necessary system changes with a click of the mouse.

This reality leads to one conclusion: PROTECT IP's DNS filtering *will* be evaded through trivial and often automated changes through easily accessible and installed software plugins. Given this

[19] http://mafiaafire.com/

strong potential for evasion, the long-term benefits of using mandated DNS filtering to combat infringement seem modest at best.

In addition, if the U.S. mandates and thereby legitimizes DNS filtering, more countries may impose their own flavor of DNS filtering. As this practice becomes more widespread, the extent to which a particular name is reachable will become a function of on which network and in which country a user sits, compromising the universality of DNS naming and thereby the "oneness" of the Internet. This situation will in turn increase the cost and challenge of developing new technologies, and reduce the reliability of the Internet as a whole. If the Internet moves towards a world in which every country is picking and choosing which domains to resolve and which to filter, the ability of American technology innovators to offer products and services around the world will decrease.

Moreover, circumvention poses risks to the security and stability of the DNS, which are explored in the following sections.

C. Circumvention Poses Performance and Security Risks

The likely circumvention techniques described above will expose users to new potential security threats. These security risks will not be limited to individuals. Banks, credit card issuers, health care providers, and others who have particular interests in security protections for data also will be affected. At the same time, a migration away from U.S.-based and ISP-provided DNS will harm U.S. network operators' ability to investigate and evaluate security threats. Intelligence and law enforcement officials who rely on high-quality network usage data afforded by centralized DNS resolution will face a similar reduction in the usefulness of DNS.[20]

1. Users Will Face Increased Cybersecurity Risk

As noted above, both users and operators of infringement sites will likely respond to DNS filtering by redirecting users' DNS settings to point outside of the United States. One cannot predict which DNS services they will use instead, but one can anticipate that some if not many of the new DNS resolvers will be well outside U.S. jurisdiction, possibly run by the same criminals running the infringement sites, and perhaps even on the same systems and hardware. This concern is not mere speculation: the use of non-U.S. DNS is already favored by malicious websites, viruses, and criminal gangs to evade U.S. law enforcement.

As a consequence of redirecting their DNS settings, users will face significantly increased security risks, as detailed below. Those risks, however, will not be obvious or well known to most users, and they will simply be unaware of the risks (and indeed, as noted above, the users may not even know that their DNS settings have been changed). Moreover, in households with shared computers, one user (say, a teenage music sharer) may redirect the DNS settings, but then those settings would carry over to when the parent later did online banking on the same computer. The teenager's redirection also could redirect banking information and put it in jeopardy. The effects of increased security vulnerability will be felt not just by users, but by U.S.

[20] A full discussion of the impact on law enforcement is outside the scope of this paper.

networks and businesses, including banks and credit card companies, which will internalize the costs of botnet disruptions, identity theft, and financial fraud.

Users on computers with redirected DNS settings will have a number of increased risks. First, operators of rogue DNS servers are less likely than major U.S. operators to support DNSSEC. Thus users who switch or are switched to such nameservers will not benefit from the security and trust DNSSEC is being implemented to provide. And the absence of support for DNSSEC may expose these users to greater risk from malicious nameserver operators.

Second, and critically, when traffic is pushed to potentially rogue servers, how will those servers handle the resolution of web and mail server lookups for military networks, U.S. banks, or social network sites used by U.S. citizens to communicate and share personal information and ideas? Circumvention has real consequences beyond evading the results of court-ordered filters. An infringement site that simply gains enough consent and cooperation from a user to shift his or her DNS resolution to the pirate site is not only insulated from the filters of PROTECT IP. The operator also gains access to *all* DNS traffic from that user:

> Every time the user seeks his bank, the pirate site has the opportunity to hijack it.
>
> Every time the user seeks an e-commerce site, the pirate site has the opportunity to impersonate it.
>
> Every email, every game, every Internet application that someone might use to be productive would potentially be exposed to manipulation.

Although some pirate operators may decide to run "honest" DNS servers in an effort to gain the trust of users, at least some of the overseas DNS servers are likely to act on their economic incentive to exploit their access to the sensitive communications of some Americans.

In the millions of DNS lookups exported from U.S. networks, many may prove innocuous, but some will fall in these sensitive categories, which will be attractive avenues for phishing and other cybercrime. In control of all of a user's DNS traffic, a rogue resolver could easily return spurious results for sensitive queries. For example, a user could be sent an identical-looking but false and criminal website pretending to be Citibank.com, allowing the operator to gain access to and empty the user's bank accounts.

If users of government or military networks violate sound security practices and redirect their DNS traffic to a non-U.S. DNS server, they could create national security risks given the sensitivity of those networks.[21] Redirection on such networks would risk providing non-U.S. networks a foothold in the DNS conversation, and the ability to monitor and manipulate resolution for potentially sensitive websites and mail servers, through denial-of-service attacks, disclosure attacks,[22] and an array of other avenues.

[21] Military information has been lost through P2P in the past; *See, e.g.,* Tim Wilson, "Army Hospital Breach May Be Result of P2P Leak," *Dark Reading*, June 3, 2008, http://www.darkreading.com/taxonomy/index/oldarticleurl?articleID=211201106.

[22] "Disclosure attack" refers to the ability of an attacker to collect target intelligence information by analyzing client behavioral and query data.

2. ISPs Will Lose Visibility into Network Security Threats

DNS data currently provides ISPs an important and accurate picture of both traffic patterns and security threats on their network, which in turn is vital for both business planning and network protection. Data gleaned from their customers' access to their DNS servers can be useful for a number of purposes. First, it can allow an ISP to identify increases and shifts in traffic, which can inform infrastructure investment, network optimizations, interconnection strategies, and peering relationships. Even more critically, monitoring DNS data is a vital part of maintaining network security. By analyzing name lookups, ISPs are able to diagnose denial-of-service attacks, identify hosts that may be part of a botnet, and identify compromised domains serving as command-and-control servers or identify subscribers who may be at risk. These analyses in turn enable network administrators to combat these problems, both by addressing malicious traffic and by providing targeted assistance to the users of infected computers.

As users increasingly turn to other DNS servers to avoid the DNS filtering, ISPs have less and less ability to manage security threats and maintain effective network operations. By losing visibility into network security threats, ISPs will be less able to identify customer computers that have been infected by a virus and come under the control of a criminal botnet. At the same time that ISPs will be less able to identify infected computers, their security offices will be less able to assist law enforcement in investigating network security attacks or data loss and exfiltration.

The reduction of customer use of an enterprise, local network operator, or ISP's DNS service will mean that more compromised computers will go unidentified and uncorrected. Furthermore, the set of attributes that need to be evaluated when a customer calls an operator help desk for support will be much more extensive, and will increase both cost and debugging complexity.

3. CDNs Would Likely Face Degraded Performance

Routing DNS traffic to offshore servers will also affect network performance within the United States, and will increase costs for ISPs. For DNS queries themselves, any delay will be minimal. However, for content delivered from Content Distribution Networks (CDNs) the impact will be more severe.

CDNs localize content delivery by distributing the same content across a number of servers on a wide range of networks. This localization reduces network congestion and decreases the load that would otherwise be put on a single server. Many CDNs use the IP address of the DNS resolver to estimate a user's location and route the user to the fastest available server. To such networks, U.S. users who have changed their DNS resolvers for all lookups will appear to the CDNs to be browsing from abroad. As a result, these users could be routed to offshore servers not just for DNS queries, but also for content, undermining precisely the benefits CDNs provide by optimizing traffic distribution to account for proximity of client and server.

Inefficient server selection would cause small delays for users, but high costs for commercial actors who must pay higher costs of latency and added network resources in order to provide the same level of service. The higher costs will negatively impact the business of both the providers of high-value, high-bandwidth (and non-infringing) content that overwhelmingly make up the customer base of CDNs, as well as the CDN operators themselves. To the extent that poor server selection results in increased traffic over international links, as is likely, it will also increase the traffic load and network congestion experienced by a wider range of network operators.

D. DNS Interdependencies Will Lead to Collateral Damage

Two likely situations ways can be identified in which DNS filtering could lead to non-targeted and perfectly innocent domains being filtered. The likelihood of such collateral damage means that mandatory DNS filtering could have far more than the desired effects, affecting the stability of large portions of the DNS.

First, it is common for different services offered by a domain to themselves have names in some other domain, so that example.com's DNS service might be provided by isp.net and its e-mail service might be provided by asp.info. This means that variation in the meaning or accessibility of asp.info or isp.net could indirectly but quite powerfully affect the usefulness of example.com. If a legitimate site points to a filtered domain for its authoritative DNS server, lookups from filtering nameservers for the legitimate domain will also fail. These dependencies are unpredictable and fluid, and extremely difficult to enumerate. When evaluating a targeted domain, it will not be apparent what other domains might point to it in their DNS records.

In addition, one IP address may support multiple domain names and websites; this practice is called "virtual hosting" and is very common. Under PROTECT IP, implementation choices are (properly) left up to DNS server operators, but unintended consequences will inevitably result. If an operator or filters the DNS traffic to and from one IP address or host, it will bring down all of the websites supported by that IP number or host. The bottom line is that the filtering of one domain name or hostname can pull down unrelated sites down across the globe.

Second, some domain names use "subdomains" to identify specific customers. For example, blogspot.com uses subdomains to support its thousands of users; blogspot.com may have customers named Larry and Sergey whose blog services are at larry.blogspot.com and sergey.blogspot.com. If Larry is an e-criminal and the subject of an action under PROTECT IP, it is possible that blogspot.com could be filtered, in which case Sergey would also be affected, although he may well have had no knowledge of Larry's misdealings. This type of collateral damage was demonstrated vividly by the ICE seizure of mooo.com, in which over 84,000 subdomains were mistakenly filtered.[23]

The authors of the paper understand that sites offering such subdomain hosting are not the target of PROTECT IP, but the possibility for such unintended filtering remains. Despite sharing a parent domain, subdomains, as well as their content, often have little or nothing to do with one another. The existence of additional subdomains may not be readily apparent upon reviewing whatever content is served at a particular subdomain, just as visiting google.com gives no indication of the existence of yahoo.com, despite the fact that the two domains share the .com top-level domain. Thus it is possible for an examination of one subdomain to conclude without ever revealing the existence of others that would be affected by a filtering order instituted in the DNS.

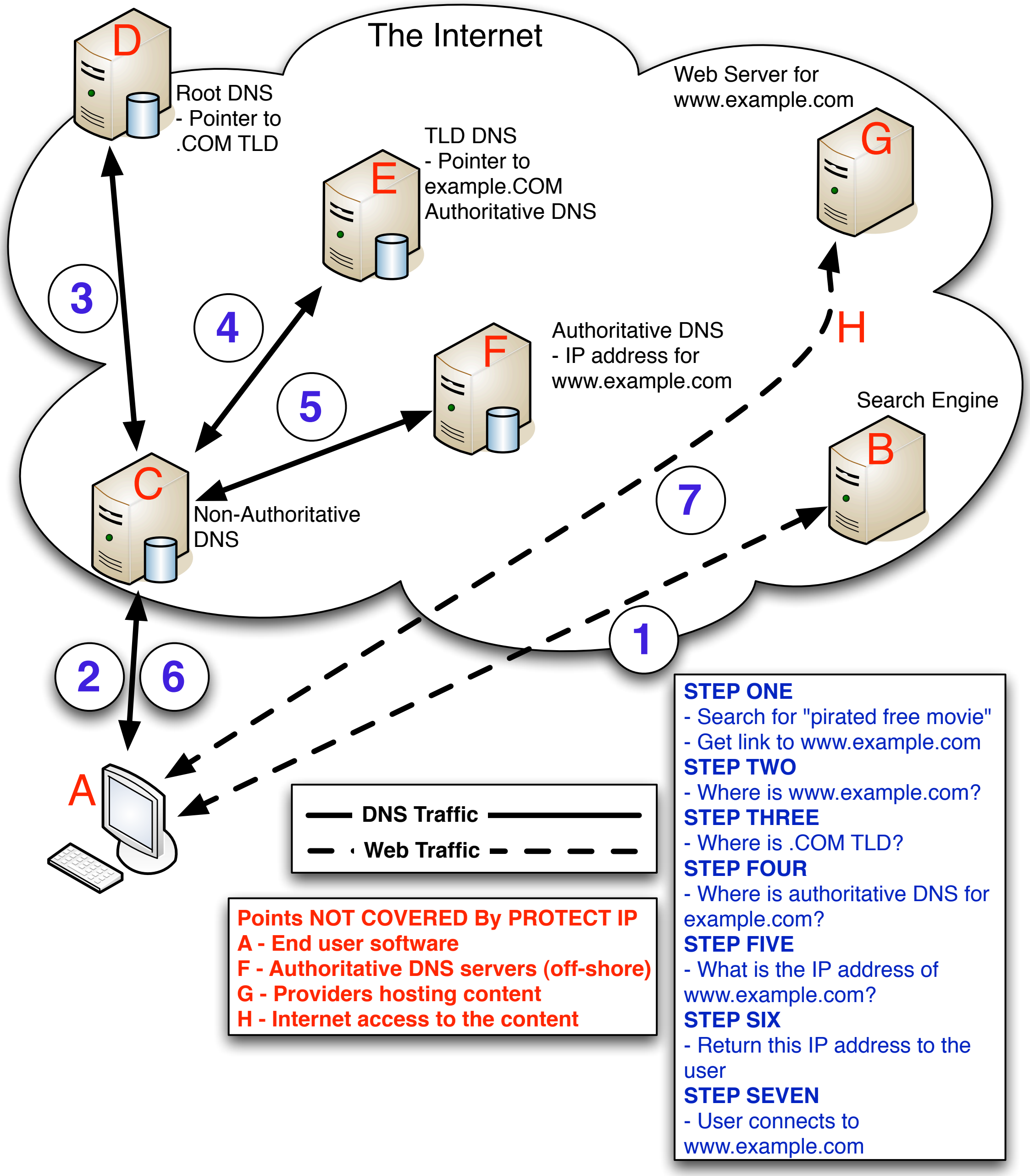
[23] Thomas Claburn, "ICE Confirms Inadvertent Web Site Seizures," *InformationWeek*, February 18, 2011, http://www.informationweek.com/news/security/vulnerabilities/229218959.

IV. Conclusion

As stated above, we strongly believe that the goals of PROTECT IP are compelling, and that intellectual property laws should be enforced against those who violate them. But as discussed in this paper, the mandated DNS filtering provisions found in the PROTECT IP Act raise very serious security and technical concerns. We believe that the goals of PROTECT IP can be accomplished without reducing DNS security and stability, through strategies such as better international cooperation on prosecutions and the other remedies contained in PROTECT IP other than DNS-related provisions. We urge Congress to reject the DNS filtering portions of the Act.

APPENDIX A

The figure below may be helpful in understanding the DNS filtering method specified in PROTECT IP



Points NOT COVERED By PROTECT IP
A - End user software
F - Authoritative DNS servers (off-shore)
G - Providers hosting content
H - Internet access to the content

STEP ONE
- Search for "pirated free movie"
- Get link to www.example.com

STEP TWO
- Where is www.example.com?

STEP THREE
- Where is .COM TLD?

STEP FOUR
- Where is authoritative DNS for example.com?

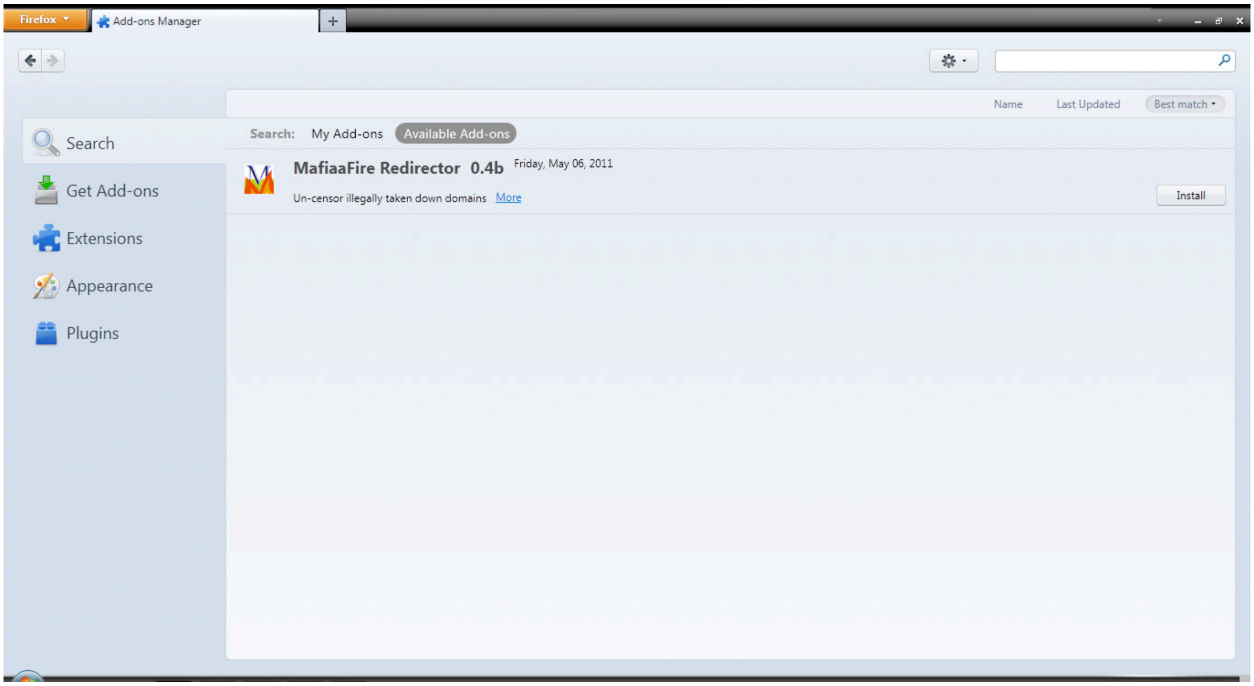
STEP FIVE
- What is the IP address of www.example.com?

STEP SIX
- Return this IP address to the user

STEP SEVEN
- User connects to www.example.com

APPENDIX B

Some browser plugins are easily installed, and would allow users to avoid the DNS filtering contemplated by PROTECT-IP. The MafiaaFire redirector, shown below, was created in direct response to domain-seizures and the introduction of COICA in 2010.



MafiaaFire Redirector 0.4b Friday, May 06, 2011

Un-censor illegally taken down domains More

Screen-captured on 05/25/11 at 10:45 a.m.

ABOUT THE AUTHORS

Steve Crocker is CEO of Shinkuro, Inc., a security-oriented consulting and development company, and has been leading Shinkuro's work on deployment of DNSSEC, the security extension to DNS. He currently serves as vice chair of the board of ICANN and served as chair of ICANN's Security and Stability Advisory Committee from its inception in 2002 until 2010. He has been active in the Internet community since 1968 when he helped define the original set of protocols for the Arpanet, founded the RFC series of publications and organized the Network Working Group, the forerunner of today's Internet Engineering Task Force (IETF). He later served as the first Area Director for Security in the IETF. Over his forty-plus years in network research, development, and management, he has been an R&D Program Manager at DARPA, senior researcher at University of Southern California's Information Sciences Institute, Director of Aerospace Corp's Computer Science Laboratory, vice president of Trusted Information Systems, co-founder, senior vice president and CTO of CyberCash, Inc. and co-founder and CEO of Longitude Systems, Inc.

David Dagon is a post-doctoral researcher at Georgia Institute of Technology studying DNS security and the malicious use of the domain resolution system. He is a co-founder of Damballa, an Internet security company providing DNS-based defense technologies. He has authored numerous peer-reviewed studies of DNS security, created patent-pending DNS security technologies, and proposed anti-poisoning protocol changes to DNS.

Dan Kaminsky has been a noted security researcher for over a decade, and has spent his career advising Fortune 500 companies such as Cisco, Avaya, and Microsoft. Dan spent three years working with Microsoft on their Vista, Server 2008, and Windows 7 releases. Dan is best known for his work finding a critical flaw in the Internet's Domain Name System (DNS), and for leading what became the largest synchronized fix to the Internet's infrastructure of all time. Of the seven Recovery Key Shareholders who possess the ability to restore the DNS root keys, Dan is the American representative. Dan is presently developing systems to reduce the cost and complexity of securing critical infrastructure.

Danny McPherson is Chief Security Officer for Verisign, Inc., where he is responsible for strategic direction, research, and innovation in infrastructure, and information security. He currently serves on the Internet Architecture Board (IAB), ICANN's Security and Stability Advisory Council, the FCC's Network Reliability and Interoperability Council (NRIC), and several other industry forums. He has been active within the Internet operations, security, research, and standards communities for nearly 20 years, and has authored a number of books and other publications related to these topics. Previously, he was CSO of Arbor Networks, and prior to that held technical leadership positions with Amber Networks, Qwest Communications, Genuity, MCI Communications, and the U.S. Army Signal Corp.

Paul Vixie founded Internet Systems Consortium in 1996 and served as ISC's President from 1996 to 2011 when he was named Chairman and Chief Scientist. Vixie was the principal author of BIND versions 4.9 to 8.2, which is the leading DNS server software in use today. He was also a principal author of RFC 1996 (DNS NOTIFY), RFC 2136 (DNS UPDATE), and RFC 2671 (EDNS), coauthor of RFC 1876 (DNS LOC), RFC 2317 (DNS for CIDR), and RFC 2845 (DNS TSIG). Vixie's other interests are Internet governance and policy, and distributed system security.