December 9th, 2011

The Honorable Patrick Leahy
U.S. Senate
Chairman, Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Charles Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Lamar Smith
U.S. House of Representatives
Chairman, Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515-6216

The Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary
House of Representatives
Washington, DC 20515

RE: S.968, Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act and H.R.3261, Stop Online Piracy Act

Dear Chairman Leahy, Ranking Member Grassley, Chairman Smith and Ranking Member Conyers:

The undersigned are DNS operators, network security professionals, and academic researchers, who jointly authored a detailed technical whitepaper[1] outlining our concerns about S. 968, the “Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act” (“PIPA”). Although our analysis has been reviewed and approved by scientists and experts in network security, such as those at the Sandia National Labs,[2] our work has met some criticism from reviewers who lack subject matter expertise and experience.[3] We believe that relevant and effective public policy must be informed by engineering consequences, not just by ideology and economics. Our goal is the health and safety of the Internet's infrastructure.

This letter discusses some of the negative reaction to our analysis, and corrects numerous misconceptions. We also reiterate the impacts of PIPA, and its House companion, H.R.3261, the Stop Online Piracy Act (“SOPA”) on the DNS infrastructure.

1) Why “Not Answering” DNS Queries Causes More Harm

In their current form, both SOPA and PIPA require ISPs to “redirect” users looking up infringing domains to a warning page. We have pointed out that, in the case of end-to-end DNSSEC resolution, redirection is an impossibility, and not cryptographically feasible.[4] While others have denied this very real mathematical limit, they have at the same time suggested that perhaps instead ISPs could simply provide other answers besides redirection.

As experts in DNS, implementors of the code running 80% of the world's DNS infrastructure, and as the co-authors of many of the core protocols for DNS and DNSSEC, we must inform that there are no protocol signals a resolver can send to a user to address the scenarios in SOPA and PIPA. Indeed, some existing responses would potentially cause some programs to stop all DNS lookups, and not just those for infringing content. When the US Government requested that we and others develop DNSSEC, it did not specify that *some* answers would not be allowed for policy reasons.

Many critics have pointed out that there are existing DNS filtering systems, such as those used for email, and typographical redirection. We will separately address these criticisms in detail, but they all suffer from a common misconception: our objection is that SOPA and PIPA conflict with DNSSEC specifically. The fact that DNS can be edited and changed for arbitrary reasons was one motivation for creating DNSSEC.[5]

Others have suggested that perhaps the ISPs could simply “not answer” the DNS queries for infringing content. This well intentioned proposal ignores the fact that a secure application expecting a secure DNS answer will not give up after a timeout. It might retry the lookup, it might try a backup DNS server, it might even restart the lookup through a proxy service. Since there is no way a secure application can know whether a timeout is due to a national anti-piracy law, it will have to assume the worst, which is: that it is under attack.

In some contexts, SOPA/PIPA-induced timeouts may also cause some applications to retry using older insecure DNS technologies. Attackers of course can exploit this in what is generally known as a “downgrade attack”[6] to cause hosts to shed security in favor of convenience.

2) Why DNSSEC Matters to the United States and the Internet

Critics of our analysis do not directly dispute our concerns about DNSSEC, and instead merely describe DNS in detail (but never DNSSEC)[7]. They offer the indirect criticism that DNSSEC is “not widely deployed”, and perhaps by implication of lesser importance. Here, it is instructive to recall the history of DNSSEC, and how it was created at the request of the US Government to serve important goals.

a) *Wide Authority Adoption.* Since 2003, every major network with a sizable population on earth has adopted DNSSEC (with the singular exception of China). On the customer side, the largest US ISP has already started offering DNSSEC validation to its users[8], and others will soon follow. DNSSEC is ***deployed*** critical Internet infrastructure used by engineers. We are also seeing growing interest and use by average users.

b) DNSSEC offers the only highly scalable secure validation system on the Internet. Existing security systems such as SSL[9] are vulnerable, subject to increasing episodes of forgery, and are commonly exploited by governments to monitor citizen activists and for industrial espionage.[10] In the wake of this technological failure, and to help keep communications confidential and authentic, the US Government[11,12] and businesses are moving forward with plans for various Internet identity systems.[13] DNSSEC is expected to play a key *infrastructure* role in securing online identity, often through various extensions to DNSSEC[14].

In conclusion, our critics have failed to address our concerns about DNSSEC, and instead describe how older DNS technology can accommodate their plans. The impossibility of the DNS redirection described by SOPA and PIPA should be addressed, but we must caution that “non-answering” brings other harms. There is no support in the DNSSEC protocol for “authentic lies”, even if government mandated.

For this reason, we do not believe the DNS provisions of SOPA and PIPA are technically workable, no matter how softened to accommodate the needs of DNSSEC.

Yours very truly,

Steve Crocker, PhD
David Dagon, PhD
Dan Kaminsky
Danny Mcpherson
Paul Vixie, PhD

[1] http://www.shinkuro.com/PROTECT%2520IP%2520Technical%2520Whitepaper%2520Final.pdf

[2] http://lofgren.house.gov/images/stories/pdf/napolitano_response_rep_lofgren_11_16_11_c.pdf

[3] Daniel Castro, “PIPA/SOPA: Responding to Critics and Finding a Path Forward”, http://www.itif.org/files/2011-pipa-sopa-respond-critics.pdf

[4] Our whitepaper, supra note 1, discusses the details. But in short, all DNSSEC answers include a cryptographic proof that the answer originated from the domain owner, and not some intercepting third party. It is impossible for any third party to forge an alternative answer, regardless of whether their intent was ill or benign. This limit comes from a mathematical imperative, and not some lack of will or commitment to solve a social harm, as our critics have suggested.

[5] One critic in particular has gone to great lengths to stress how DNS filtering can work with DNS, and even illustrates how the DNS system works. See Castro, supra note 3. Yet this analysis nowhere describes how DNSSEC works, or makes the assertion the DNS filtering is compatible with DNSSEC. We recognize in this fundamental error a need to better educate the public about DNSSEC.

[6] Matt Bishop, "Computer Security: Art and Science", Addison-Wesley, 2002.

[7] See, Castro, supra note 3.

[8] See, e.g., http://blog.comcast.com/2011/12/dnssec-deployment-update.html

[9] T. Dierks and E. Rescorla “RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2”, August 2008.

[10] See Keven O'Brien, “Hacking in Netherlands Points to Weak Spot in Web Security”, Sept. 12, 2011, http://www.nytimes.com/2011/09/13/technology/hacking-in-netherlands-points-to-weak-spot-in-web-security.html

[11] "National Strategy to Secure Cyberspace", Feb. 2003, http://www.dhs.gov/files/publications/editorial_0329.shtm

[12] K. Evans, "Security the Federal Government's Domain Name System Infrastructure", OMB mandate M-08-23, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf

[13] See, e.g., “NSTIC: The Identity Ecosystem: Use Examples”, http://www.nist.gov/nstic/identity-ecosystem.html

[14] See, e.g., “DANE – DNS-Based Authentication of Named Entities”, https://www.ietf.org/mailman/listinfo/dane