Internet Engineers' Letter Urging Amendment of the PROTECT-IP Act

October 12, 2011

To Members of the United States Senate:

We urge the modification of S. 968, the PROTECT-IP Act of 2011, to remove the provision requiring that domestic Internet service providers filter their Domain Name Service ("DNS") results to protect brand and copyright owners against online infringement.

We are engineers who have spent our careers working in and with the Internet's domain name system at a nuts-and-bolts level. We have developed or collaborated on key technical standards that are fundamental to the functioning of the Internet. We are recognized as leading experts in this particular field of technology. Ordinarily we do not get involved in legislative debates, but we believe that our background leaves us ideally situated to offer a full and realistic evaluation of the likely consequences of certain provisions of S. 968.

We recognize and strongly support the rights of brand and copyright owners and we believe that S. 968's provisions curtailing the use of domestic advertising and payment networks by infringing web sites are well considered and will prove effective. However, the filtration of DNS results required by S. 968 would prove both costly and ineffective, and would have serious negative side effects.

PROTECT-IP's Proposed DNS Filtering Is Not Technically Feasible

As drafted, S. 968 calls for DNS editing that is not technically feasible, and incompatible with Internet DNS security extensions (also known as DNSSEC or Secure DNS). These security features have been under development for more than fifteen years with heavy investment by both US industry and US Government, and are now being deployed globally. ICANN has signed the DNS root zone, the U.S. Government has signed .EDU, .GOV and .MIL, large generic top level domains including dot-COM, dot-NET, and dot-ORG are signed, and almost 80 of countries have signed their top-level domains[1].

We stand now on the threshold of the next era in Internet security infrastructure, in which new and more secure applications from e-shopping to e-banking can can rely on Secure DNS as their foundation for online identity. If not amended to remove the DNS filtering provision, S. 968 would demand that ISPs choose between deploying Secure DNS and ignoring court-ordered DNS filtering, or forgoing Secure DNS in order to comply with the law.

Recent letters[2] and online posts[3,4] by proponents of S. 968 have misstated key facts about DNS and Secure DNS. A white paper[5] by the authors of this letter provides a comprehensive technical critique of the DNS provisions of S. 968, endorsed by the editorial boards of prominent national newspapers[6,7].

PROTECT-IP's Proposed DNS Filtering Would Be Ineffective

Even assuming that domestic ISPs make the high initial and ongoing investment in name server filtering required by S. 968, ISPs cannot force their customers to use their name servers. Any user can avoid such filtering by using another name server, possibly located off-shore and not subject to US law. These off-shore name servers will be capable of redirecting web traffic to malicious sites including fake banks and search engines.

By moving information-rich DNS lookup data offshore, users would create risk for the whole US information economy, not just for themselves. And the effort and expertise required to change a user's DNS settings is trivial, often reduced to "one click" or even completely automated.

PROTECT-IP's DNS Filtering Would Bring Negative Side Effects

Proponents of the DNS provisions of S. 968 assert that this proposed legislation would have no impact on Internet infrastructure. The facts about Secure DNS say otherwise. Secure DNS means being able to verify the integrity and source of DNS data, e.g., allowing a user to know whether it has reached their bank or an impostor site. DNS filtering asks DNS servers to "lie" by providing incorrect responses. If Secure DNS is deployed, a user's DNS client will know when it is being lied to. But it won't know whether the lie is the result of court-ordered DNS filtering or criminal interference with the user's DNS lookup. The inability to distinguish legitimate DNS diversions from malicious ones will make it impossible to use DNSSEC as a platform to build robust security protections.

Any comparison of S. 968's DNS provisions to current filtering technologies such as parental controls or spam or malware blocking is inapt. These technologies are wanted by, and indeed installed and operated by, the end users themselves. When provided by ISPs, users do not complain or change their name servers because they are happy with the filtering. It should also be noted that when ISPs deploy Secure DNS, they will no longer be able to use the current filtering technologies. As described above, DNS filtering and Secure DNS are mutually incompatible.

Requiring ISPs to deploy DNS filtering is futile and dangerous. The mere threat of S.968's filtering provision has resulted in the marketing in this country of fast, easy and zero-cost tools to change users' name servers. Just as we predicted in our white paper, there are now numerous evasive DNS services which promise to evade any mandated DNS blocking[8,9,10]. Annually, there are 58 billion page visits to sites dedicated to infringing activities which represents an enormous level of demand. To satisfy that demand, users will change their name servers.

PROTECT-IP's DNS Provisions Should Be Dropped

As stated, S. 968's goals are laudable, and its provisions regarding domestic advertising and payment networks are reasonable. However, no good and much harm can come from the DNS provision of S. 968 as currently written, and we urge that this provision be dropped when the bill is considered by the full Senate.

Signed,

Steve Crocker, Ph.D. – co-creator of the original ARPANET protocols; former Internet Engineering Task Force (IETF) security area director, former Internet Architecture Board member, former Internet Society board member; member of ICANN security and stability advisory committee.

David Dagon, Ph.D. – author of numerous peer-reviewed studies of Secure DNS; co-founder of Internet security company providing DNS-based defense technologies; inventor of proposed anti-poisoning technology for DNS.

Dan Kaminsky – noted security researcher best known for his work finding a critical flaw in the Internet's Domain Name System (DNS); of the seven Recovery Key Shareholders who possess the ability to restore the DNS root keys, Dan is the American representative.

Danny McPherson – Chief Security Officer, Verisign, Inc.; member FCC CSRIC; appointed member Internet Architecture Board; author of numerous security and engineering studies, Internet RFCs, and several books; member of ICANN security and stability advisory committee.

Paul Vixie, Ph.D. – founder of Internet Systems Consortium (ISC), operator of "F" root DNS name server, publisher of BIND DNS software system; IETF DNS protocol contributor; member of ARIN Board of Trustees; member of ICANN security and stability advisory committee.

1 DNSSEC Deployment Project, http://www.dnssec-deployment.org/
2 IFTA, et al, “To the Members of the United States Senate”, http://www.mpaa.org/resources/f63d5736-4e36-49fb-a452-586b23d24b04.pdf
3 George Ou, “DNS Filtering is Essential to the Internet”, http://www.hightechforum.org/dns-filtering-is-essential-to-the- internet/
4 Michael O'Leary, “PROTECT-IP Letter from Law Professors Didn't Do its Homework”, http://blog.mpaa.org/BlogOS/post/2011/07/07/PROTECT-IP-Letter-from-Law-Professors-Did-Not-Do-its- Homework.aspx
5 Steve Crocker, David Dagon, Dan Kaminsky, Danny McPherson, and Paul Vixie, “Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT-IP Act”, http://www.shinkuro.com/PROTECT%20IP%20Technical%20Whitepaper%20Final.pdf
6 The Los Angeles Times, “Policing the Internet”, http://www.latimes.com/news/opinion/opinionla/la-ed-protectip-20110607,0,2415749.story
7 The New York Times, “Internet Piracy and How to Stop It”, http://www.nytimes.com/2011/06/09/opinion/09thu1.html
8 Domain Incite, “Pirates set up domain seizure workaround”, http://domainincite.com/pirates-set-up-domain-seizure- workaround/
9 Telecomix DNS, http://dns.telecomix.org/
10 Dot-P2P, http://dot-p2p.org/