December 14, 2011

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

Dear Chairman Smith:

I appreciate the opportunity to express my concerns about and opposition to the managers' amendment to the Stop Online Piracy Act (SOPA) and, in particular, the "technological solutions" related to the Domain Name System (DNS) and search engines.

By way of background, I am a Vice President and the Chief Internet Evangelist for Google. I also serve as a Fellow of the Institute for Electrical and Electronics Engineers (IEEE), the Association for Computing Machinery (ACM), the American Association for the Advancement of Science (AAAS), and the American Academy of Arts and Sciences, and I am a member of the National Academy of Engineering.

I have held positions at MCI, the Corporation for National Research Initiatives, Stanford University, UCLA and IBM. Until 2007 I served as chairman of the board of the Internet Corporation for Assigned Names and Numbers (ICANN) and I was the founding president of the Internet Society.

As one of the "fathers of the Internet" and as a computer scientist I care deeply about issues relating to the Internet's infrastructure. In that spirit I wish to join the Internet and cybersecurity experts who have already expressed concern about the original version of SOPA's DNS provisions. Former NSA general counsel Stewart Baker, Sandia National Laboratories, small businesses such as OpenDNS, inter-industry groups such as the Messaging Anti-Abuse Working Group (MAAWG), five leading DNS engineers (Steve Crocker, David Dagon, Dan Kaminsky, Danny McPherson, and Paul Vixie), and dozens of individual security experts have detailed these concerns in previous letters.

Unfortunately, the amendments to SOPA do not resolve the fundamental flaws in this legislation; the bill will still undermine cybersecurity including the robust implementation of DNS Security Extensions, known more commonly as DNSSEC.

Section 102(e)(2)(i) continues to require service providers to block access to sites. While

that provision no longer *mandates* DNS blocking in order to accomplish that goal, it still *permits* falsifying IP addresses in response to domain name resolution requests. Any response that provides a false IP address triggers potential damage to the intent of DNSSEC.

If these changes were meant to dispel the concerns of the security community, then they fall far short of the mark. The Section 102(e)(2)(ii) "safe harbor" effectively singles out the manipulation of DNS as the preferred mechanism for blocking access to sites. A key presumption in the Internet design and architecture is the global consistency of DNS lookup responses.

I continue to have concerns regarding the efficacy and wisdom of this legislation. First, attempts to manipulate DNS will reduce the utility of DNS as our chief mechanism for locating sites, and encourage abusers to adopt alternative mechanisms, such as IP address lists. Second, clients of the infringing content can readily change their DNS settings to utilize offshore DNS resolvers. Third, sites dedicated to infringement have many options for evading these measures, such as registering multiple domain names with offshore registries in order to stay ahead of court orders. Fourth, falsifying responses to domain name resolution requests will compromise the "downgrade resistance" of next-generation improvements to DNSSEC, because systems that do not receive a signed answer from a resolver will fall back to accepting unsigned responses to resolve a domain name.

Thus, even with the proposed manager's amendment, SOPA's site-blocking provisions remain problematic. They would undermine the architecture of the Internet and obstruct the 15 year effort by the public and private sectors to improve cybersecurity through implementation of DNSSEC, a critical set of extensions designed to address security vulnerabilities in the DNS.

This collateral damage of SOPA would be particularly regrettable because site blocking or redirection mechanisms are unlikely to make a significant dent in the availability of infringing material and counterfeits online, given that DNS manipulation can be defeated by simply choosing an offshore DNS resolution provider, maintaining one's own local DNS cache or using direct IP address references.

The search engine remedy also suffers from the fact that it will not be effective in preventing users' access to illegal, offshore websites. A congressional "tech mandate" on search engines to delete a domain name from search results does not result in the website disappearing. Users can and do today find their way to these websites largely without the help of search engines. Relative to the questionable efficacy of this proposed remedy, requiring search engines to delete a domain name begins a worldwide arms

race of unprecedented "censorship" of the Web.

Rather than continuing to promote ineffective and harmful "technical" solutions as those found in the managers' amendment to SOPA, I urge Congress to pursue a more tailored, effective approach, such as the "follow-the-money" tactic. Such an approach would cut off funding mechanisms to rogue foreign sites by withholding their ability to generate advertising revenue and their ability to have payments processed.

Sincerely,

Vint Cerf

cc: Members of the House Judiciary Committee